Orgaan van de

Nederlandse Vereniging

van Wiskundeleraren

EUCLIDES

Vakblad voor de wiskundeleraar

jaargang 72

1996-1997 nov./dec.

3

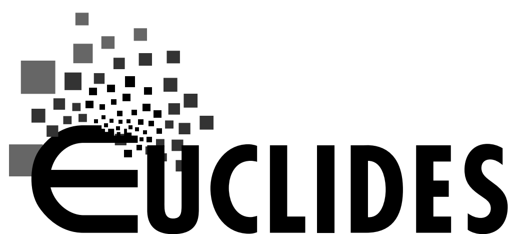




Dynamische systemen

Wereldrecord getallen kraken met behulp van World Wide Web

Oproep nieuwe redactieleden



Euclides is het orgaan van de Nederlandse Vereniging van Wiskundeleraren. Het blad verschijnt 8 maal per verenigingsjaar.

Redactie

Artikelen/mededelingen

Artikelen en mededelingen naar:
Kees Hoogland
Gen. Cronjéstraat 79 rood
2021 JC Haarlem.

Richtlijnen voor aanlevering:
- goede afdruk met illustraties/foto's/formules op juiste plaats of goed in de tekst aangegeven.
- platte tekst op diskette: WP of ASCII
- illustraties/foto's/formules op aparte vellen: genummerd, zwart/wit, scherp contrast.

Nadere richtlijnen worden op verzoek toegezonden.

Nederlandse Vereniging van Wiskundeleraren

Voorzitter
dr. J. van Lint
Spiekerbrink 25
8034 RA Zwolle
tel. 038-4539985
Secretaris
W. Kuipers
Burg. Bijleveldsingel 38
8052 AP Hattem
tel. 038-4447017
Ledenadministratie
Mw. N. van Bemmel-Hendriks
De Schalm 19
8251 LB Dronten
tel. 0321-312543

Contributie per ver. jaar: ƒ70,00
Studentleden: ƒ47,50
Leden van de VVWL: ƒ50,00
Lidmaatschap zonder Euclides: ƒ50,00
Betaling geschiedt per acceptgiro.
Nieuwe leden geven zich op bij de ledenadministratie.
Opzeggingen vóór 1 juli.

Abonnementen niet-leden

Abonnementen gelden steeds vanaf het eerstvolgende nummer.
Abonnementsprijs voor personen: ƒ80,00 per jaar. Voor instituten en scholen: ƒ240,00 per jaar.
Betaling geschiedt per acceptgiro.
Losse nummers op aanvraag leverbaar voor ƒ20,00.
Opzeggingen vóór 1 juli.

Advertenties

Informatie, prijsopgave en inzending:
C. Hoogsteder, Prins Mauritshof 4
7061 WR Terborg, tel. 0315-324337
of naar:
L. Bozuwa, Merwekade 90
3311 TH Dordecht, tel. 078-6145522.

Adresgegevens auteurs

CWI
Kruislaan 413
1098 SJ Amsterdam

J. Hop
Molenweg 13
3849 RK Hierden

M. Kollenveld
Leeuwendaallaan 43
2281 GK Rijswijk

H.N. Pot
Tournoysveld 67
3443 ER Woerden

V.E. Schmidt
Verlengde Grachtstraat 43
9717 GE Groningen

E.M. van de Vrie
Disselhof 16
6418 JM Heerlen

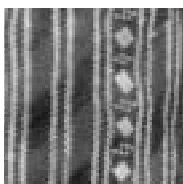
H. Wisbrun
O. Zijds Achterburgwal 137
1012 DG Amsterdam

G. Zwaneveld
Bieslanderweg 18
6213 AJ Maasstricht

Inhoud


120


124


137



van de redactietafel

Na het themanummer van de vorige keer heeft u nu weer een meer regulier nummer voor u, met daarin hopelijk voor elk wat wils: wiskunde, verslagen, mto, wiskunde in de Derde Wereld, werkbladen, recreatie en de kalender. De redactie heeft er overigens geen enkel bezwaar tegen dat u, als lezer, actiever laat horen aan wat voor soort berichtgeving in Euclides behoefte bestaat.

Uw mening

Een manier om uw mening in Euclides over het voetlicht te krijgen zijn korte ingezonden brieven. Al enkele keren is dat aangekondigd in dit stukje. De inzendingen stromen nog niet bepaald binnen. Terwijl op jaarvergaderingen, examenbesprekingen, regionale bijeenkomsten, nascholing en in docentenkamers toch stellig de indruk gekregen kan worden, dat vele collega's uitgesproken meningen hebben over de ontwikkelingen in het wiskundeonderwijs in Nederland. De redactie reserveert alvast een halve bladzijde ruimte voor uw mening. Misschien geeft de volgende alinea al wat ammunitie.

4 vwo en 4 havo/B

Na de eerste maanden in 4 vwo en 4 havo wiskunde B wordt het duidelijk dat een soepele aansluiting op de nieuwe onderbouw geen vanzelfsprekendheid is. De meningen daarover die 'rondzingen' zijn zeer divers. Ze lopen uiteen van: '*Het wiskundeonderwijs in Nederland is niks meer*' tot '*Ze hebben er meer plezier in, maar ik moet ze nog wel even duidelijk maken dat algebraïsche vaardigheden op dit moment ook belangrijk zijn.*'
Daar tussen in liggen natuurlijk ook allerlei meningen: '*Het wiskunde leren in de onderbouw is nog lang niet uitgekristalliseerd voor havo en vwo. Zeker in de derde klas moeten nog de goede accenten gelegd worden.*' Of: '*Er zijn docenten in de bovenbouw die nog geen goed zicht hebben op wat de leerlingen in de onderbouw nu precies geleerd hebben. Er is alleen oog voor wat minder is geworden.*'
Verontrustend is dat leerlingen in de vierde klas er op worden aangesproken dat ze sommige zaken minder of niet meer kunnen. Alsof zij verantwoordelijk zijn voor de inhoud van het leerplan.
De redactie is geïnteresseerd in uw mening over deze en andere zaken. Brieven voor het volgende nummer moeten wel voor 10 december binnen zijn.

En verder

Nog een paar losse puntjes:
- In de kalender is een lijstje opgenomen met mogelijk voor wiskundedocenten interessante Internet-bladzijden. Aanvullingen daarop zijn welkom.
- Op 20 september jongstleden is op een feestelijke bijeenkomst het Freudenthal instituut door het ministerie, bij monde van mevrouw Netelenbos, aangemerkt als nationaal expertisecentrum rekenen/wiskunde. Dat is een felicitatie vanaf deze plaats waard.
- Er is een nieuw concept-leerplan voor het mbo verschenen. Daarvan in dit nummer een aankondiging. In latere nummers zullen we daarover ongetwijfeld meer vernemen. Ook van die kant is er dus serieuze aandacht voor de aansluiting.

Ten slotte

Op de voorlaatste bladzijde staat een oproep voor nieuwe redactieleden van Euclides. Dit blad komt natuurlijk niet vanzelf tot stand. Het is bekend dat scholen in toenemende mate de aandacht en energie vragen van docenten voor schoolzaken. Maar het is ook bekend dat een sterke beroepsvereniging met een goede spreekbuis essentieel is om toekomstige veranderingen te volgen, bij te stellen en onderwijsbaar te houden. Een uitgelezen kans om naast de schoolwereld kennis te nemen van en mee te werken aan de wondere wereld van het wiskundeonderwijs in Nederland. U misschien?

Kees Hoogland

Dynamische systemen

Victor Schmidt

Aanleiding

Op de jaarvergadering/studiedag van onze vereniging van 1994 hield professor F. Takens van de Rijksuniversiteit Groningen een voordracht over chaostheorie in het kader van het studiethema ‘Van exploreren naar bewijzen’. Wie het verhaal zich nog weet te herinneren, zal kunnen beamen dat het onderwerp weliswaar interessant was, maar de spreker zich wat verloor in wiskundige stellingen en definities. Tijdens een nascholingscursus op het gebied van toepassingen van informatica in bedrijfsorganisaties die ik jaren geleden eens heb gevolgd, hield een andere Groningse hoogleraar over hetzelfde onderwerp een tamelijk inzichtelijk verhaal. Aan de hand van een expliciete oplossing van een bepaalde vergelijking wist professor Simons het verschijnsel chaos aan de cursusdeelnemers duidelijk te maken. In een drietal artikelen zal ik de gedachtengang van Simons volgen en vervolgens een uitstap maken naar de zogenaamde kleine stelling van Fermat uit de getaltheorie.

Dynamische systemen

Veel verschijnselen in de natuur, de economie, sociologie, kortom de reële wereld kunnen als een zogenaamd dynamisch systeem beschouwd worden. Een dergelijk systeem bevindt zich op zeker moment in een bepaalde toestand. Het systeem heet dynamisch, omdat zijn toestand in de tijd verandert. Een dynamisch systeem wordt discreet genoemd als de momenten waarop de toestand van het systeem zich wijzigt, van elkaar te onderscheiden zijn. Is dat niet het geval, dan is er sprake van een continu dynamisch systeem. We zullen ons in het vervolg beperken tot eerstgenoemde categorie systemen.

Veel wetenschappelijke disciplines bestuderen dynamische systemen zoals bijvoorbeeld de bevolking in een bepaalde regio, de economie van een land, of het weer op een bepaalde plaats. Vaak wordt er van het systeem een (kwantitatief) model gemaakt, waarmee het systeem, of bepaalde aspecten daarvan, beschreven kunnen worden. Zo kan men de bevolking in een regio modelleren door haar omvang en de economie door grootheden als nationaal inkomen, consumptie, besparingen en investeringen. Het weer op een bepaalde plek kan worden beschreven met luchtdruk, temperatuur, luchtvochtigheid, windsnelheid en windrichting ter plaatse.
Naast een model voor het systeem zelf worden er ook modellen ontwikkeld voor het gedrag van het systeem in opeenvolgende tijdsintervallen. Aan de hand van deze gedragsmodellen kunnen er voorspellingen gedaan worden over de toekomstige toestanden van het dynamische systeem. Met behulp van een gedragsmodel kan worden nagegaan of het systeem bijvoorbeeld de neiging heeft naar een vaste toestand te groeien of een vaste cyclus van verschillende toestanden te doorlopen. Bovendien kan bepaald worden in hoeverre een systeem bestand is tegen verstoringen van buitenaf.

Gedragsmodellen

Als de toestand van een systeem zich in een tijdsinterval met nummer n laat beschrijven door een toestandsvariabele x_n, dan bestaat het gedragsmodel voor dit systeem uit een vergelijking van de vorm

$$x_n = f(x_{n-1}, x_{n-2}, \ldots)$$

In het geval het systeem met behulp van meer dan één variabele beschreven wordt, is x_n een vector en f een functie die op vectoren werkt en een vector als resultaat geeft. We laten deze mogelijkheid in het vervolg achterwege.
Het model zegt dat de toestand van het systeem in een zeker tijdsinterval bepaald wordt door de toestanden van het systeem in een aantal voorafgaande tijdsintervallen. De afhankelijkheid wordt beschreven met de functie f. We zullen ons in het vervolg beperken tot systemen waarvan de toestand in een tijdsinterval uitsluitend afhangt van de toestand in het onmiddellijk daaraan voorafgaande interval. De gedragsvergelijking heeft dan de vorm

$$x_n = f(x_{n-1})$$

Aan de hand van deze vergelijking is het mogelijk onderzoek te doen naar de opeenvolgende toestanden van het systeem, mits de begintoestand x_0 bekend is. Gezocht kan worden naar toestanden die niet meer in de tijd veranderen. Andere toestanden keren na een

vast aantal tijdsintervallen telkens terug. Ook kan bekeken worden in hoeverre deze bijzondere situaties in de toekomst in stand blijven.
Kortom, we zullen onderzoek doen naar *evenwichtsoplossingen*, *periodieke oplossingen* en de *stabiliteit* daarvan.

Lineaire modellen

De meest eenvoudige gedragsmodellen zijn lineair, hetgeen betekent dat de gedragsfunctie f lineair is. Dergelijke modellen komen vaak voor, meestal omdat de opsteller van het model niet over voldoende informatie beschikt om aan te nemen dat f niet lineair is. Daarnaast zijn de oplossingen van een lineair model eenvoudig te bepalen. We bekijken als voorbeeld het gedragsmodel

$$x_n = 0{,}5x_{n-1} + 0{,}2$$

Dit model kent een evenwichtsoplossing, die kan worden berekend door in de gedragsvergelijking x_n en x_{n-1} aan elkaar gelijk te stellen en kortweg x te noemen. Het resultaat is

$$x = 0{,}5x + 0{,}2$$

Hieruit volgt dat $x = 0{,}4$. Heeft de toestandsvariabele als beginwaarde 0,4, dan houdt zij deze waarde.

Een lineair model heeft geen periodieke oplossingen. Voor een oplossing met een periode van bijvoorbeeld 2 moet voor elke waarde van n gelden dat $x_n = x_{n-2}$ en bovendien $x_n \neq x_{n-1}$. Uit de gedragsvergelijking volgt dat $x_{n-1} = 0{,}5x_{n-2} + 0{,}2$ en dus dat

$$x_n = 0{,}5x_{n-1} + 0{,}2 = 0{,}5(0{,}5x_{n-2} + 0{,}2) + 0{,}2$$
$$= 0{,}25x_{n-2} + 0{,}3$$

Stellen we $x_n = x_{n-2} = x$, dan blijkt dat $x = 0{,}4$. Dit is echter de evenwichtsoplossing, zodat niet voldaan is aan $x_n \neq x_{n-1}$. Andere periodieke oplossingen zijn niet aanwezig.

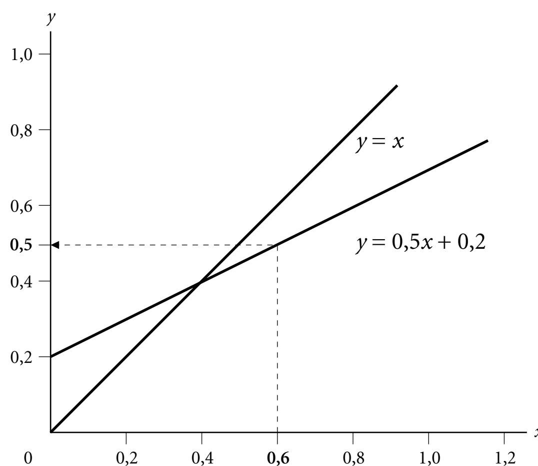
De stabiliteit

Is de evenwichtsoplossing $x = 0{,}4$ stabiel? Een antwoord op deze vraag kan gegeven worden door x_n te schrijven als $0{,}4 + u_n$ en te onderzoeken hoe u_n zich gedraagt als u_0 dicht bij 0 ligt. Voor u_n geldt dan

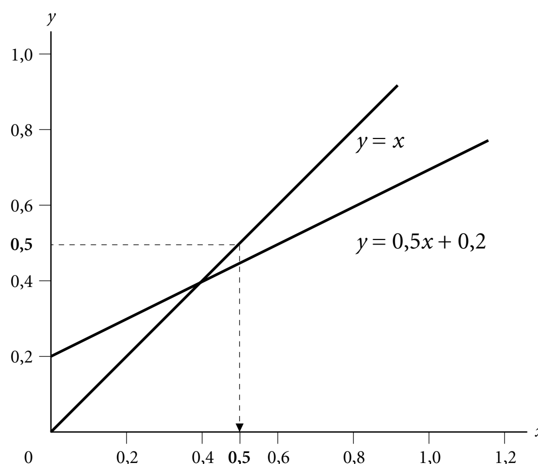
$$u_n = 0{,}5u_{n-1}$$

Duidelijk is dat de rij u_n tot 0 nadert, ongeacht de waarde van u_0. Daarmee is niet alleen aangetoond dat de evenwichtsoplossing stabiel is en bestand is tegen een willekeurig kleine verstoring, maar dat élke begintoestand uiteindelijk evolueert naar de evenwichtstoestand $x = 0{,}4$.

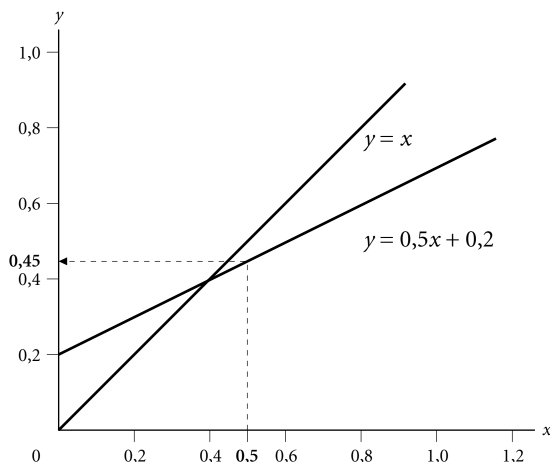
Dit verschijnsel kan in een figuur uitgebeeld worden. Daartoe wordt in een assenstelsel de grafiek van f en de lijn met vergelijking $y = x$ getekend. Met behulp van de grafiek kan, gegeven een beginwaarde van de toestandsvariabele op de X-as, de waarde ervan in tijdsinterval 1 op de Y-as worden afgelezen. Willen we de waarde van de toestandsvariabele in tijdsinterval 2 met behulp van de grafiek aflezen, dan moet eerst de waarde in tijdsinterval 1 op de X-as worden opgezocht. Dat is mogelijk door de eerder gevonden waarde op de Y-as op de X-as terug te lezen met behulp van de lijn met vergelijking $y = x$. Vervolgens kunnen we met behulp van de grafiek de waarde in tijdsinterval 2 opzoeken. In figuren 1a tot en met 1c zijn de beschreven stappen uitgevoerd bij een beginwaarde van 0,6. In figuur 2 is het procédé een aantal malen herhaald. Daarbij is de bewerkingsgang vereenvoudigd weergegeven.



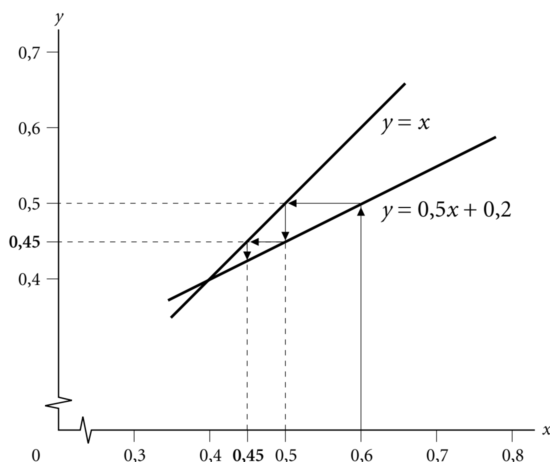
figuur 1a



figuur 1b



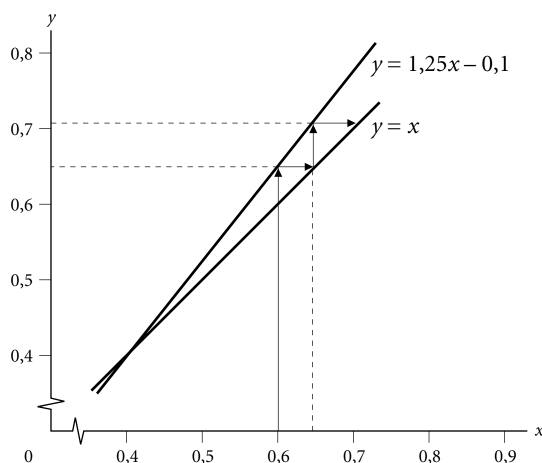
figuur 1c



figuur 2

Duidelijk is dat de opeenvolgende punten op de grafiek van *f* naar het snijpunt van de grafiek en de lijn $y = x$ naderen. Daaruit blijkt nogmaals dat de oplossing met beginwaarde 0,6 naar de evenwichtsoplossing evolueert.

Niet altijd is de evenwichtsoplossing bij een lineair model stabiel. In figuur 3 is een gedragsmodel weergegeven waarin elke oplossing met een beginwaarde ongelijk aan 0,4 van de evenwichtsoplossing wegloopt.



figuur 3

Het al dan niet stabiel zijn van een oplossing van een lineair model wordt bepaald door de richtingscoëfficiënt van de grafiek van *f*. Is die coëfficiënt in absolute waarde kleiner dan 1, dan is stabiliteit verzekerd. Sterker nog, élke oplossing groeit naar de evenwichtsoplossing. Het systeem is bestand tegen elke verstoring van buitenaf, hoe groot ook. Als de absolute waarde van de richtingscoëffiënt groter is dan 1, dan is de evenwichtsoplossing instabiel.

Niet-lineaire modellen

In sommige gevallen blijkt een lineair model te eenvoudig te zijn om het gedrag van een dynamisch systeem te beschrijven. De voorspellingen die op basis van een dergelijk model gedaan worden vertonen bijvoorbeeld te veel afwijkingen met het daadwerkelijk waargenomen gedrag van het systeem, zonder dat daar achteraf een aanwijsbare reden voor bestaat. De veronderstelling dat de gedragsfunctie *f* lineair is, is te eenvoudig en daarom zal een de opsteller van een model op zoek gaan naar ingewikkelder gedragsfuncties.

Een voorbeeld: Jarenlang is verondersteld dat de omvang van een populatie individuen (mensen, dieren of planten) zich volgens een lineair model gedraagt. Het aantal individuen groeit in dat geval exponentieel in de tijd en dat bleek te kloppen met waarnemingen door demografen. Biologen ontdekten echter dat in situaties waarin de hoeveelheid leefruimte en voedsel beperkt zijn, deze groei afgeremd wordt. De tot dan toe geldende hypothese van de lineariteit van de gedragsfunctie was niet langer houdbaar en men veronderstelde dat de gedragsfunctie *f* van de graad 2 was. Geavanceerde gedragsmodellen voor de omvang van een populatie hebben de onderstaande vorm.

$$x_n = \mu x_{n-1}(1 - x_{n-1})$$

In deze gedragsvergelijking stelt *xn* de omvang van de bevolking voor als fractie van een theoretische bovengrens. x_n neemt waarden aan tussen 0 en 1. Als x_{n-1} dicht bij 0 ligt is de invloed van de factor $1 - x_{n-1}$ verwaarloosbaar en lijkt de groei inderdaad exponentieel te verlopen, dat wil zeggen: x_n is dan bijna een exponentiële functie van *n*.
De parameter μ is tenminste gelijk aan 1 (anders verdwijnt de bevolking op lange termijn en dat is in dit kader niet interessant) en ten hoogste gelijk aan 4.

Afstand

Een aardige vraag is het bepalen van de afstand van een punt A tot een gegeven parabool.

Een voorbeeld:

Bepaal de afstand van het punt $A\,(0, 6)$ tot de parabool $8y = x^2$.

We minimaliseren het kwadraat van de afstand van A tot een punt (x, y) van de parabool.

minimaliseer
$f(x, y) = x^2 + (y - 6)^2$
$x^2 = 8y$ dus

minimaliseer
$g(y) = 8y + (y - 6)^2$

$\frac{dg}{dy} = 8 + 2(y - 6) = 0 \rightarrow$

$y = 2 \rightarrow x = 4 \vee x = -4$

De gevraagde afstand is $4\sqrt{2}$.

We nemen $A(0, 2)$

We minimaliseren nu
$f(x, y) = x^2 + (y - 2)^2$ en dus

$g(y) = 8y + (y - 2)^2$

$\frac{dg}{dy} = 8 + 2(y - 2) = 0 \rightarrow$

$y = -2 \rightarrow x^2 = -16$

Hetgeen geen reële waarde voor x oplevert. De afstand van A tot de parabool lijkt te zijn verdwenen.

Alleen als $\mu \leq 4$ staat vast dat, als x_{n-1} tussen 0 en 1 ligt, ook x_n tussen 0 en 1 valt, hetgeen blijkt door het maximum van de functie $f(x) = \mu x(1 - x)$ te berekenen. Dit maximum is namelijk $\frac{1}{4}\mu$.
We zullen dit voorbeeld in het vervolg verder uitdiepen.

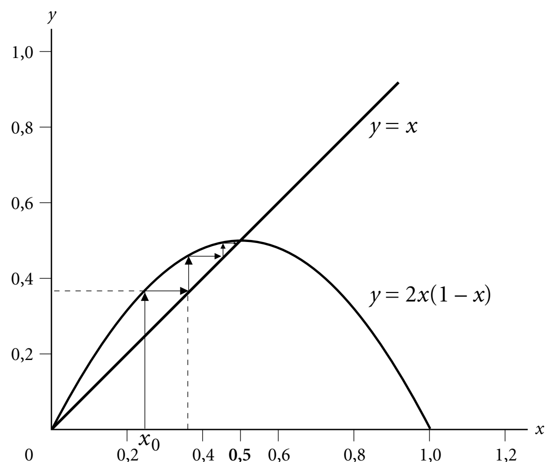
De evenwichtsoplossing

Het bevolkingsmodel heeft voor elke waarde van μ die binnen de aangegeven grenzen valt, een evenwichtsoplossing. Door in de gedragsvergelijking zowel x_n als x_{n-1} gelijk te stellen aan x vinden we

$$x = \mu x(1 - x)$$

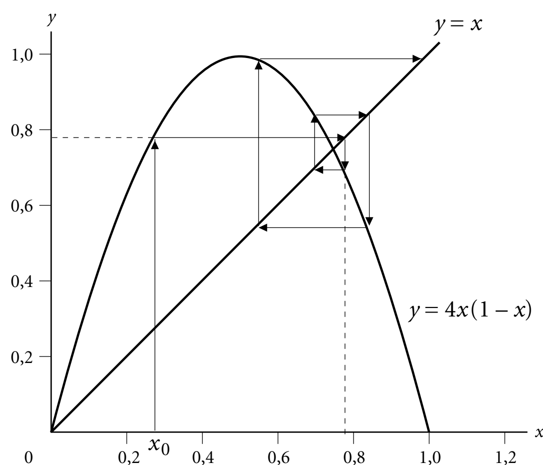
Naast $x = 0$ heeft deze vergelijking als oplossing $x = 1 - 1/\mu$. We laten $x = 0$ buiten beschouwing en zullen $x = 1 - 1/\mu$ als de evenwichtsoplossing beschouwen. Bovendien zullen we de situatie met $\mu = 1$ achterwege laten, omdat voor deze waarde van μ de evenwichtsoplossing $x = 1 - 1/\mu$ gelijk is aan 0.

Om de stabiliteit van de evenwichtsoplossing te onderzoeken kunnen wederom in één figuur de grafiek van f en de lijn $y = x$ getekend worden. In de figuren 4 en 5 is het resultaat te zien bij $\mu = 2$ en bij $\mu = 4$. Tevens is de stabiliteitsanalyse bij een beginwaarde x_0 weergegeven.



figuur 4

In de figuren zien we dat voor $\mu = 2$ de evenwichtsoplossing 0,5 stabiel is en dat voor $\mu = 4$ de evenwichtsoplossing 0,75 juist niet stabiel is. De vraag rijst met welke berekening de stabiliteit van de evenwichtstoestand bepaald kan worden. De evenwichtstoestand blijkt alleen dan stabiel te zijn als de richtingscoëffiënt van de raaklijn aan de grafiek van f in het snijpunt met de lijn $y = x$ in absolute waarde kleiner is dan 1. Zonder in te gaan op de bewijsvoering is dit resultaat aan de hand van de volgende redenering te begrijpen.



figuur 5

Bij een *lineair model* wordt de stabiliteit van de evenwichtstoestand bepaald door de richtingscoëfficiënt van de grafiek van de gedragsfunctie *f* (waarvan de grafiek een rechte lijn is). Als deze richtingscoëfficiënt in absolute waarde kleiner is dan 1, is er stabiliteit. Omdat de richtingscoëffiënt van de raaklijn aan de grafiek van een *niet-lineaire functie* als een veralgemenisering gezien kan worden van het begrip richtingscoëfficiënt van een rechte lijn, is het gestelde in lijn met het voorgaande.

Aan de hand van de bovenstaande gedachtengang kunnen de waarden van μ gevonden worden, waarvoor de evenwichtstoestand stabiel is. Daartoe moet $f'(x)$ voor $x = 1 - 1/\mu$ tussen -1 en 1 liggen. Nu is

$$f'(x) = \mu(1 - 2x) \quad \text{en dus} \quad f'(1 - 1/\mu) = -\mu + 2$$

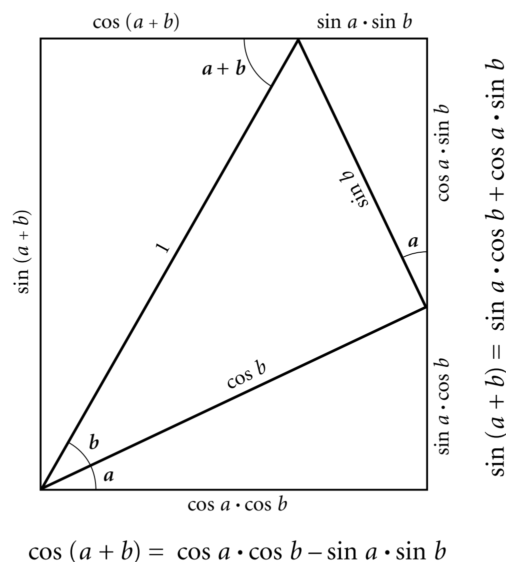
Deze waarde van $f'(1 - 1/\mu)$ valt tussen -1 en 1 als $1 < \mu < 3$. Voor deze waarden van μ is de evenwichtstoestand stabiel. Zoals Takens uiteenzette, is bij deze waarden van μ de evenwichtstoestand niet alleen ongevoelig voor een kleine verstoring, maar zelfs voor elke verstoring. We werken dit laatste hier niet verder uit.

Chaos

Als de parameter $\mu \geq 3$ treedt er een situatie op, die met *chaos* wordt aangeduid. De evenwichtstoestand is niet meer stabiel en er blijkt ruimte te zijn voor periodieke oplossingen. Ook is er geen ordentelijke evolutie in de zin dat, als x_n en x_m dicht bij elkaar liggen, voor elke *k* ook x_{n+k} en x_{m+k} dicht bij elkaar liggen.
Het moge duidelijk zijn dat voorspellingen op lange termijn in een zich chaotisch gedragend systeem niet mogelijk zijn, tenzij de voorspellers zich bedienen van de statistiek.
In het volgend artikel zullen we voor $\mu = 4$ de evenwichtsoplossing en de periodieke oplossingen van het gedragsmodel beschrijven. Voor deze waarde van de parameter kan de gedragsvergelijking met behulp van goniometrische functies opgelost worden.

Een grafische herleiding van sin(a + b) en cos(a + b)

Hessel Pot



Het idee om de somformules voor de sinus en de cosinus op een dergelijke manier te visualiseren is natuurlijk niet nieuw. Er staat tenslotte niets anders dan het volgende:
- in het midden bevindt zich de definitie-driehoek voor de sinus en de cosinus van een hoek ter grootte *b*;
- onderaan en rechtsboven bevindt zich de definitie-driehoek voor de sinus en de cosinus van een hoek ter grootte *a*;
- links bevindt zich de definitie-driehoek voor de sinus en de cosinus van een hoek ter grootte $a + b$.

Ik probeerde de grafische mogelijkheden die een figuur biedt, hier zoveel mogelijk te benutten en te optimaliseren. Ik wilde ook elke tekst vermijden.
Kan het beter? Vast wel.

Huiswerk
a. Maak iets analoogs voor $\sin(a - b)$ en $\cos(a - b)$.
b. Kan of mag de figuur, zònder verdere tekst, gelden als *bewijs* voor de beide somformules?

P.S. Een kladversie van deze figuur stond al eerder in Euclides (mei 1981).

INTERVIEW

‘De vraag: waarom heb je wiskunde eigenlijk nodig? komt de laatste jaren niet meer voor’

Nico Derks, 43 jaar, is vanaf 1976 in het onderwijs, eerst als natuurkunde- en wiskundeleraar in de onderbouw, de laatste 10 jaar alleen nog als wiskundeleraar. Sinds 1992 geeft hij ook bovenbouwlessen. Vanaf 1977 is hij ononderbroken verbonden aan het St. Maartenscollege te Maastricht. De school is een scholengemeenschap mavo, havo, vwo.

In welk soort klassen geef je het liefst les?
Mijn voorkeur gaat uit naar de onderbouw en in de bovenbouw iets meer naar havo (A of B) dan naar het vwo. De onderbouw vanwege het grote enthousiasme van de leerlingen. Ik werk graag aan het bijbrengen van een goede wiskundige denk- en werkhouding, en dat kan daar nog steeds heel goed. De bovenbouw havo boeit me meer vanwege het werken met in het algemeen spontane, gemakkelijke en ongecompliceerde leerlingen.

Vind je de leerlingen erg veranderd gedurende je loopbaan als leraar?
De leerlingen zijn veranderd, maar de leraren, de school en de samenleving ook. De veranderingen in de afgelopen 15 tot 20 jaar zijn moeilijk als positief of negatief te beoordelen, omdat de veranderingen heel geleidelijk gaan en je zelf ook verandert. Ik noem een paar opvallende veranderingen: brugklasleerlingen zijn nog steeds enthousiast, maar hebben soms toch een wat ander gedrag dan vroeger. Zo zijn er bij klassikale instructie of bij huiswerk bespreken veel meer leerlingen die de informatie wel beluisteren maar niet in hun schrift vastleggen en daardoor vaak dezelfde fouten blijven maken. Verder is de rekenvaardigheid, het begrijpend lezen en de tijd dat ze zich kunnen concentreren gemiddeld genomen lager. De durf, de openheid, de verbale vaardigheden en de spontaniteit zijn groter. In de middenklassen haken de leerlingen niet meer of pas veel later af bij het vak wiskunde. In het verleden leverden deze voor wiskunde afgehaakte leerlingen nogal eens problemen op. In deze klassen heeft het nieuwe programma enkele verbeteringen gebracht onder andere door de grotere variatie in de onderwerpen, de meer contextrijke aanpak, de minder abstracte opzet en de grotere mogelijkheden tot zelfwerkzaamheid van de leerlingen. Typerend in dit opzicht is dat de vroeger veel gestelde vraag: waarvoor heb je wiskunde eigenlijk nodig? en de opmerking na een les: sorry, meneer, maar de les was ook weer zo saai! de laatste jaren niet meer voorkomen.

Wat vind je belangrijk in je wiskundelesssen?
In de lessen ligt bij mij de nadruk op het verwerven van inzicht, het aankweken van goede vaardigheden, het leggen van verbanden tussen de onderdelen en het leren van een goede werkhouding. Dit laatste kost trouwens steeds meer energie en tijd.



Om een voorbeeld te noemen: in de onderbouw schrijven veel leerlingen nog steeds een soort 'steno'- wiskunde, dat wil zeggen, uitsluitend antwoorden of zeer summiere of bijna niet te volgen verklaringen. Het leukste en het belangrijkste voor mij is dat ik blijf proberen mijn eigen enthousiasme voor wiskunde over te brengen op de leerlingen.

De basisvorming is nu een aantal jaren bezig. Hoe beoordeel je die voor wiskunde?
De basisvorming is bij wiskunde samengevallen met een gedeeltelijk ben er bijvoorbeeld niet zo gelukkig mee dat vanaf het begin en altijd het rekenapparaat gebruikt wordt. Ook het absolute verbod op het gebruiken van variabelen in de brugklas en het minimale rekenen met breuken kan mij niet bekoren. Een belangrijke verbetering is het weer terugkeren van een groter stuk meetkunde in de onderbouw. In dit verband is het misschien aardig om op te merken dat onze school als één van de laatste scholen het systeem van twee cijfers in de onderbouw, één voor meetkunde en één voor algebra, tot 1983 heeft gehandhaafd.

schillen tussen de leerlingen zijn erg groot. Het vinden van goede contexten bij proefwerken en bij eindexamenopgaven begint steeds moeilijker te worden. Maar dat was te verwachten. De opbouw in de examenopgaven begint inderdaad redelijk standaard te worden. Een verhaal met een gegeven formule en/of grafiek, enkele waarden invullen, vervolgens iets aflezen in de grafiek (het eerste tijdvak van het laatste examen moest dat liefst 10 keer in een grafiek op log-papier), dan een deel van de formule vervangen door een andere uitdrukking en de nieuwe formule uit-



nieuw onderbouw programma en mavo-eindexamen. Gezien de ontwikkeling van het wiskundeonderwijs in Nederland van de laatste jaren, was het min of meer een logische stap. Voor mij en mijn collega's, als gebruikers van Moderne Wiskunde, waren de veranderingen niet zo heel groot. Toch ben ik niet onverdeeld tevreden. De gemaakte keuzen bij het samenstellen van de leerstof in W12-16 zijn voor onze leerlingen niet altijd verbeteringen geweest. Ik

De laatste tijd hoor je meer en meer kritiek op wiskunde A. Het eindexamen begint zich teveel te standaardiseren met een te lang verhaal en opgaven op een te laag niveau: alleen wat rekenen of aflezen uit een grafiek. Wat is jouw mening?
Mijn ervaringen met wiskunde A zijn nog niet zo uitgebreid. Tot nu toe deel ik die kritiek niet. Wel heb ik de indruk dat de dubbelkeuze wiskunde A en B op vwo in de lessen niet gelukkig uitvalt. De niveau- en tempover-

werken tot een gegeven vorm, het maximum bepalen, enz. Meer variatie en diepgang levert waarschijnlijk te veel problemen op voor met name de leerlingen met uitsluitend wiskunde A in het pakket. Nee, van mij mag het examen juist voor deze leerlingen zo blijven. Maar wel: de dubbelkeuze verbieden, of minstens zoveel mogelijk ontmoedigen.

Bert Zwaneveld

Adviesleerplan wiskunde MTO is uit!

Jacob Hop

Inleiding

In dit artikel wil ik kort ingaan op de inhoud van het adviesleerplan voor het MTO. Nadat in het voorjaar van 1995 nieuwe eindtermen voor de vakken wiskunde en natuurkunde opgesteld waren, was de ontwikkeling van een leerplan een logisch gevolg hierop. Toen ook de financiën hiervoor beschikbaar kwamen, kon de gevormde leerplangroep, bestaande uit diverse docenten uit het MTO onder leiding van E. Payens (HvU) en Hans Wisbrun (SLO), in de eerste helft van 1996 aan de slag. Uit eindtermen een consistent leerplan maken is een uitdaging, die door de groep met enthousiasme aangegaan is.
In augustus is dit adviesleerplan opgeleverd door de SLO. Dit leerplan, in dit artikel zal ik voor de leesbaarheid het woord advies verder weglaten, is in september 1996 naar alle scholen gestuurd. Voor mij was het de eerste keer dat ik deel uitmaakte van een leerplangroep. Ik heb echter wel meegewerkt aan de totstandkoming van de eindtermen waarop het leerplan gebaseerd is.
Zoals in de toelichting op de eindtermen vermeld staat moet het nieuwe leerplan voldoen aan een aantal voorwaarden:

- aansluiting bij de nieuwe examenprogramma's wiskunde voor vbo/mavo C/D;
- toepassing van wiskundige vaardigheden en kennis op technisch relevante gebieden;
- behandeling van de leerstof vanuit contexten.

Kortom, het isolement waarin wiskunde binnen het MTO verzeild is geraakt, moet doorbroken worden. Nu het leerplan op tafel ligt, kunnen we ons de vraag stellen of aan bovengestelde criteria voldaan wordt. De leerplangroep heeft dat onderzocht middels een aantal voor dat doel ontwikkelde voorbeeldopgaven. Deze zijn ter verduidelijking toegevoegd aan het leerplan. Voordat ik over ga tot het bespreken van zo'n opgave, eerst iets over de indeling en verdeling van de leerstof.

Verdeling van de leerstof

Na ampele overwegingen is de conclusie van de groep dat de eindtermen redelijkerwijs in de daarvoor gestelde tijd gehaald kunnen worden. In de opzet is gekozen voor een indeling van de lesstof in blokken van ongeveer 8 à 9 lesweken. De reden hiervoor is dat veel MBO-scholen op dit moment zo'n blokindeling van het schooljaar kennen. Bovendien lijkt de lesstof goed te verdelen over min of meer afgeronde eenheden van 8 à 9 lesweken.
Om aan de doelstelling van toepasbaarheid in de techniek te voldoen, is een behoorlijk deel van het leerplan ingeruimd voor opleidingsafhankelijke onderwerpen. Deze blokken lopen overigens voor de verschillende studierichtingen in tijd parallel. Zie hiervoor onderstaand schema.

Een voorbeeldopgave

Terugkomend op de eerder genoemde voorwaarden waaraan het leerplan moet voldoen, neem ik één van de bijgevoegde opgaven als voorbeeld.
Wat in de eerste plaats opvalt is het grote verschil met een willekeurige

Schema wiskunde

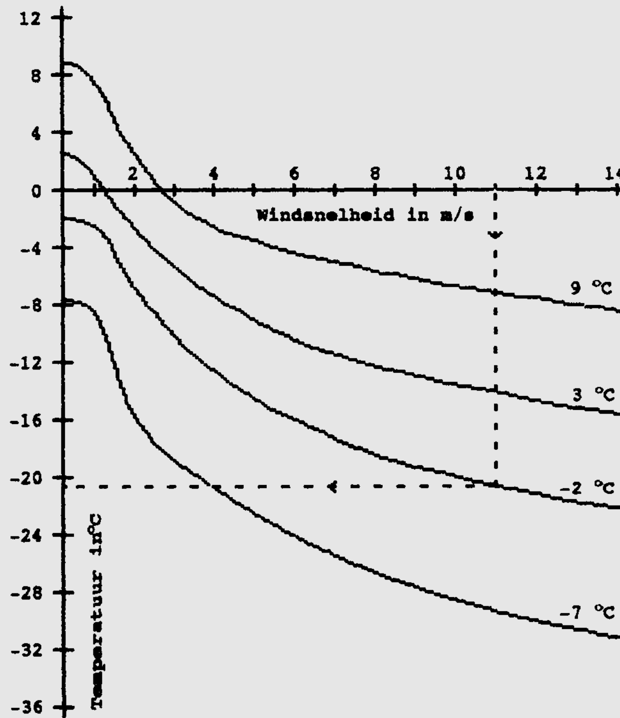
	Semester 1		Semester 2		Semester 3	
	Blok 1	Blok 2	Blok 3	Blok 4	Blok 5	Blok 6
B	INTRODUCTIE EN REKENEN	GRAFIEKEN EN VERBANDEN	Ruimtemeetkunde / Gonio en Meetk.	Logaritmen en Gonio / Gonio en Meetk.	Ruimtemeetkunde	FORMULES EN VERBANDEN
E	INTRODUCTIE EN REKENEN	GRAFIEKEN EN VERBANDEN	Gonio en Talstelsels / Gonio en Meetk.	Logaritmen en Gonio / Gonio en Meetk.	Gonio en Complexe getallen	FORMULES EN VERBANDEN
W	INTRODUCTIE EN REKENEN	GRAFIEKEN EN VERBANDEN	Ruimtemeetkunde / Gonio en Meetk.	Algebra en Gonio / Gonio en Meetk.	Ruimtemeetkunde en Schakelalgebra	FORMULES EN VERBANDEN

B = Bouwkunde
E = Elektrotechniek
W = Werktuigbouwkunde

(grijs vak) = Afdelings*af*hankelijk
(wit vak) = Afdelings*on*afhankelijk

Gevoelstemperatuur

Hoe harder het waait, des te kouder is het voor je gevoel.
Hiernaast zie je een grafische weergave van het verband tussen de werkelijke temperatuur en de gevoelstemperatuur als functie van de windsnelheid. De figuur bevat een bundel krommen, voor diverse buitentemperaturen één. De stippellijn in de figuur laat zien dat bij een buitentemperatuur van -2 °C en een windsnelheid van 11 m/s het voor je gevoel maar liefst ca. -20 °C is!



Bestudeer de figuur en beantwoord daarna de vragen.

a. Als er geen verschil zou zijn tussen de werkelijke- en de gevoelstemperatuur, hoe zouden de vier grafieken er dan uitzien ?
b. Iemand zegt 'Volgens mij vriest het wel een graad of twee.' De werkelijke temperatuur bedraagt echter +9 °C. Wat zal ongeveer de windsnelheid zijn geweest?
c. Maak een grafiek van de gevoelstemperatuur als functie van de werkelijke temperatuur bij een windsnelheid van 3 m/s.
d. Ga door interpolatie na hoe groot de windsnelheid is als bij een buitentemperatuur van -4 °C de gevoelstemperatuur -18 °C is.
e. Geef grofweg aan bij welke windsnelheid de invloed van een plotselinge windvlaag het sterkst voelbaar is. Motiveer je antwoord.

opgave uit een huidig wiskunde-MTO-boek.
De leerlingen krijgen een plaatje voorgeschoteld met een aantal realistische grafieken. Bovendien moet voordat aan de werkelijke opgave begonnen kan worden een behoorlijk stuk tekst worden doorgewerkt. Vraag a en b zijn gericht op de interpretatie van de grafieken. Wat staat er eigenlijk en hoe verloopt de grafiek? Het globale kenmerk van deze vragen is een uitgangspunt van het nieuwe leerplan. Interpretatie van gegeven situaties en het kunnen begrijpen van gegevens zijn belangrijke vaardigheden voor een MTO-leerling.
In de overige vragen spelen vaardigheden met betrekking tot interpoleren, produceren van grafieken en motiveren van antwoorden een belangrijke rol. Niet het uiteindelijke antwoord is het belangrijkste, doch het proces om tot het antwoord te komen staat voorop.

Aansluiting op vbo/mavo C/D

Om deze opgave nader te beschouwen aan de hand van de drie eerder genoemde voorwaarden het volgende. Het zal een ieder die kennis genomen heeft van de nieuwe vbo/mavo C/D programma's wiskunde duidelijk zijn dat deze opgave geheel in de lijn van dit programma ligt. Deze context is niet direct een voorbeeld van een technisch toepasbare context. Het is echter wel zo dat in de techniek bundels van grafieken vaak voorkomen en dan door leerlingen begrepen moeten worden. De herkenbaarheid van het probleem 'gevoelstemperatuur' is echter dermate groot dat deze opgave goed kan functioneren in een omgeving naast technische contexten. Bovendien leent deze opgave zich uitermate goed voor het trainen van een nog niet eerder genoemd aspect: samenwerking. Ik kan me bij deze opgave levendig voorstellen hoe een groepje leerlingen al samenwerkend tot een goede oplossing komt. Dit aspect van samenwerking en zelfstandigheid van de leerling wordt in het leerplan niet met name genoemd, maar het leerplan geeft een goede aanzet in die richting. Uiteindelijk zal de praktijk uitwijzen welke veranderingen zullen plaatsvinden in de klassen; het leerplan biedt voldoende mogelijkheden voor een wiskunde die van deze tijd is.

Verslag

Regionale bijeenkomsten

Bert Zwaneveld

Zoals de laatste jaren gebruikelijk organiseerde ook dit voorjaar het bestuur van de NVvW vier regionale bijeenkomsten voor de leden. Er waren vier middagwerkgroepen en vijf vooravondwerkgroepen waaruit er steeds één te kiezen was. In totaal hebben ongeveer 200 collega's de vier bijeenkomsten in Zwolle, Amsterdam, Eindhoven en Rotterdam bezocht. Hier volgt een korte impressie van drie werkgroepen.



Ruimtemeetkunde met de ogen dicht of via een CD-ROM?

Er werd niet overal even enthousiast gereageerd, maar in Eindhoven is de kennismaking met een bij de lerarenopleiding in Windesheim ontwikkelde CD-ROM positief ontvangen. De bedoeling van deze CD-ROM is leerlingen in de toekomstige bovenbouw zelfstandig problemen, theorie en vaardigheden uit de ruimtemeetkunde te laten leren. De positieve ontvangst kwam mede door het enthousiasme van de inleider/ontwikkelaar Nellie Verhoef. Het belangrijkste was de discussie met de zaal over vragen als: Voor wie is het bedoeld? Hoe kun je zoiets gebruiken naast je leerboek? Waarom zou zoiets nu beter werken dan wat we nu doen? Hoe duur is dat nu (ontwikkelkosten en kosten afspeelapparatuur)? Hoe waren de reacties van de leerlingen?

Het niet volledig uitontwikkelde programma met foto's en filmpjes gaat over een meisje dat in haar eentje een zeilreis op zee maakt. Er zijn opgaven en mogelijkheden om tekeningen te maken. Ruimtemeetkundige concepten als standhoek worden visueel op een originele wijze ondersteund. Het programma bevat informatie over de achterliggende theorie en de gebruikelijke algoritmen. De bedoeling is dat kleine groepjes leerlingen in de bovenbouw havo het programma zelfstandig doorwerken. Het programma is niet bedoeld als vervanging voor het cursorische onderwijs, eerder als ondersteuning voor leerlingen die daar niet genoeg aan hebben en de stof nog eens op andere manier gepresenteerd willen krijgen. Leidend beginsel bij het ontwerpen was dat ruimtemeetkunde met gebruik van reële problemen beoefend kan worden. Achterliggend was de gedachte dat ruimtelijk inzicht wellicht beter aangebracht kan worden door objecten van alle kanten te bekijken. In het programma is dat vormgegeven door objecten te laten draaien zodat ze vanuit een ander gezichtspunt bekeken kunnen worden. Op het beeldscherm wordt uiteraard alles in een of andere tweedimensionale projectie weergegeven. Door de technische mogelijkheden ziet het er echter zeer driedimensionaal uit.
De ontwikkelaar meldde dat haar eerste ervaringen met leerlingen positief zijn, beter, zoals ze zelf zei, dan toen ze hen ruimtemeetkunde

liet bedrijven in het donker met de ogen dicht. In het najaar zal een grootscheeps experiment in de omgeving van Zwolle plaats vinden.

Een nieuwe leerling, een nieuw leerplan

Vanuit het mto-platform was er een werkgroep over de komende veranderingen in het wiskundeonderwijs in het mto. Veel informatie heeft de lezer al eerder in Euclides aangetroffen. Opmerkelijk is dat voor de leerlingen die vanuit het mto naar het hto doorstromen een concept-programma is vastgesteld dat opvallend grote gelijkenis vertoont met wat de vakontwikkelgroep voor het havo-profiel Natuur & Techniek heeft opgesteld. Als u echter weet dat het Freudenthal instituut een belangrijke bijdrage heeft geleverd, is het wat minder opmerkelijk. Interessant waren de discussies. De discussie over het basismodule (dat is het programma dat voor het hele mto gelijk is, het zit vòòr de beroepsprofilering in de eerste drie of vier semesters) had voor de doorgewinterde havo/vwo-leraar veel herkenbaars. De volgende vragen kwamen aan de orde: Waarom wiskunde in contexten? Waar halen we de proefwerken voor dergelijke wiskunde vandaan? Is het resultaat van een dergelijk programma nu echt wel beter dan het bestaande? Hoe gaat het met de aansluiting op het nieuwe mavo/vbo-examen? Hoe reageer ik als mijn collega's uit andere vakken vragen hoe het met de algebraïsche vaardigheden zit? Beschikken deze leerlingen wel over voldoende taalvaardigheid om de 'verpakkingsverhalen' te doorgronden? Over het vinden van contexten, die de leerlingen aanspreken, waren de inleiders, Tom Goris en Michel van Glabbeek, optimistisch: die moeten aan de beroepsprofielen van het mto ontleend kunnen worden, en zij lieten niet onaardige pogingen zien. Uw verslaggever was niet verbaasd te horen dat het Cito wel belangstelling heeft om een rol te spelen bij de afsluiting van deze basismodule. Verder werd er over de invoering gesproken. Het lijkt erop dat de uitgevers van wiskundemethoden voor deze sector nog niet erg wakker zijn. Voorziene invoering in 1998 lijkt dan ook een illusie. Maar vanaf 1997 komen er wel leerlingen aan die in vbo/mavo volgens een vergelijkbaar programma zijn opgeleid. En die zouden dan verder moeten gaan met een 'ouderwets' programma dat vooral op het beheersen van de algoritmen uit is en niet op het toepassen in relevante gebieden. Kortom: nog veel onduidelijkheid, maar de enthousiaste deelnemers aan het mto-platform laten zich niet ontmoedigen en roepen de aanwezige mto-docenten op actief hun steentjes aan hun platform te gaan bijdragen.



Wiskundelessen met Derive

Onder leiding van Agnes Verweij en andere enthousiaste Derive-gebruikers was er een werkgroep waarin de deelnemers zelf aan de slag konden met Derive. Bij elke regionale bijeenkomst trok deze werkgroep de grootste belangstelling. Met behulp van een practicum leerden de deelnemers het programma bedienen, en tegelijk kregen zij een aardig overzicht over de belangrijkste mogelijkheden. En dat liep gesmeerd. Aardig was het om het schoolonderzoek te zien dat één van de inleiders door zijn leerlingen met Derive had laten maken. Toch is er wel een bedenking bij zowel het practicum als het schoolonderzoek. Afgezien van een onderzoek naar het al dan niet priem zijn van een groot getal, waren het allemaal opgaven die elke wiskundedocent en elke leerling van de bovenbouw met pen en papier zonder Derive, zou moeten kunnen maken. Een pakket als Derive is niet bedoeld voor zulke opgaven, maar eerder voor opgaven die met de hand zeer bewerkelijk of tijdrovend zijn. Verder kan het programma behulpzaam zijn bij het oplossen van problemen, bijvoorbeeld in een verkennende fase. Dit soort mogelijkheden zijn belangrijker dan nagaan of Derive standaardopgaven correct kan oplossen.

RSA-130 = 18070 82088 68740 48059 51656 16440 59055 66278 10251 67694 01349 17012 70214 50056 66254 02440 48387 34112 75908 12303 37178 18879 66563 18201 32148 80557
=
45534 49864 67359 72188 40368 68972 74408 86435 63012 63205 06960 09990 44599
x
39685 99945 95974 54290 16112 61628 83786 06757 64491 12810 06483 25551 57243

Nieuw wereldrecord getallen kraken *met behulp van* World Wide Web

CWI[1]

RSA-130, een getal van 130 cijfers, is ontbonden in factoren: twee priemgetallen van 65 cijfers. De laatste schakel van dit wapenfeit werd gedurende de Paasdagen uitgevoerd op het Centrum voor Wiskunde en Informatica (CWI) te Amsterdam. Opmerkelijk hierbij was, naast het gebruik van een nieuwe methode (de Number Field Sieve), de inschakeling van Internet bij het verzamelen van de benodigde gegevens. Deze combinatie van nieuwe wiskunde en technische hulpmiddelen lijkt het ontbinden van grote getallen in een stroomversnelling te brengen en het is dan ook de vraag of het nieuwe record lang stand zal houden. Dit is van direct belang voor de bescherming van vertrouwelijke gegevens, want een der belangrijkste cryptografische technieken (RSA) berust op de praktische onmogelijkheid om bepaalde grote getallen in factoren te ontbinden. Het 'kraken' van RSA-130 is onderdeel van het door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek NWO gefinancierde promotieonderzoek van drs. Marije Elkenbracht-Huizing, dat wordt uitgevoerd op het CWI en de Rijksuniversiteit Leiden.

Eeuwenlang was ontbinden in factoren uitsluitend een recreatief probleem. De introductie in 1978 door Rivest, Shamir en Adleman van het RSA-cryptosysteem -een methode om informatie onleesbaar te maken voor onbevoegden- bracht hier verandering in. Bij deze methode kiest iedere gebruiker twee priemgetallen: getallen die alleen deelbaar zijn door één en door zichzelf. Hij maakt het product van beide priemgetallen bekend, maar houdt de priemgetallen zelf geheim. Iedereen die hem een boodschap wil sturen vercijfert deze boodschap met behulp van het bekend gemaakte product. Alleen met de priemgetallen zelf kan de oorspronkelijke boodschap weer worden teruggevonden. Daarmee hangt de veiligheid van deze methode af van de mogelijkheid van anderen om het product in factoren te ontbinden.
Met kleine getallen kunnen we zoiets nog wel uit het hoofd, bijvoorbeeld $33 = 3 \times 11$. Met grotere getallen echter moeten we er al gauw de computer bijhalen en getallen met honderden cijfers zijn met de huidige stand van de technologie ook voor de krachtigste computer meestal niet te 'kraken'. In de praktijk gebruikt men thans priemgetallen van zo'n 100 cijfers.

Licenties en producten gebaseerd op de RSA-methode worden verkocht door het Amerikaanse bedrijf RSA Data Security, Inc. Om goed zicht te houden op de kracht van ontbindingsmethoden heeft dit bedrijf een zogenaamde RSA Challenge List opgesteld van getallen die een prijs opleveren wanneer ze worden ontbonden (voor RSA-130 is dat 13.000 dollar). Na RSA-100 in 1991, RSA-110 in 1992 en RSA-120 in 1993 was het nu de beurt aan RSA-130.

Van het getal RSA-130 was bekend dat de ontbinding bestaat uit slechts twee priemfactoren van 65 cijfers. Op dit moment is de snelste methode om zo'n getal te ontbinden de enkele jaren geleden gepubliceerde Number Field Sieve (zie kader), gebaseerd op een idee van John Pollard. Een moderne PC met

Ontbinden in factoren met de Number Field Sieve

Het basisidee van zowel de Number Field Sieve (NFS) als de Quadratic Sieve (QS) methode stamt van Pierre de Fermat (1601-1665). De waarschijnlijk oudste manier om een getal in factoren te ontbinden is de lijst van priemgetallen 2, 3, 5, … te nemen en na te gaan welke priemgetallen dat getal delen. Fermat had een ander idee. Neem een oneven samengesteld getal $N = r \times s$, bijvoorbeeld 7×11. Fermat merkte op dat 7×11 is te schrijven als het verschil van twee kwadraten $x^2 - y^2$, met $x = (11 + 7)/2$ en $y = (11 - 7)/2$ dus: $77 = 9^2 - 2^2$. Als omgekeerd r en s onbekend zijn, dan is het dus de kunst om getallen x en y te vinden zodanig dat $N = x^2 - y^2$. Uit de gevonden x en y kunnen we dan de factoren $x + y$ en $x - y$ van N vinden. Meer in het algemeen kunnen we proberen getallen x en y te vinden zodat $x^2 - y^2$ een veelvoud is van N. Zo is bijvoorbeeld $160^2 - 27^2 = 25600 - 729 = 323 \times \mathbf{77}$.

We kunnen $x^2 - y^2$ ook schrijven als $(x + y) \times (x - y)$. We hopen dan dat één van de factoren van 77 een deler is van $x + y$ en dat de andere factor een deler is van $x - y$. Dat gebeurt in het voorbeeld:

$(160 + 27) \times (160 - 27) = 187 \times 133 = (\mathbf{11} \times 17) \times (\mathbf{7} \times 19)$.

We kunnen nu een priemfactor van 77 vinden door de grootste gemeenschappelijke deler (ggd) van 77 en $x + y$ te berekenen. Daarvoor is een zeer snel algoritme beschikbaar, reeds aangegeven door de Griekse wiskundige Euclides in de 4*e* eeuw voor Christus. Deze vindt de ggd van twee getallen zonder die eerst in priemfactoren te ontbinden. Zo vinden we ggd(77, 187) = 11 als priemfactor van 77.

Relaties

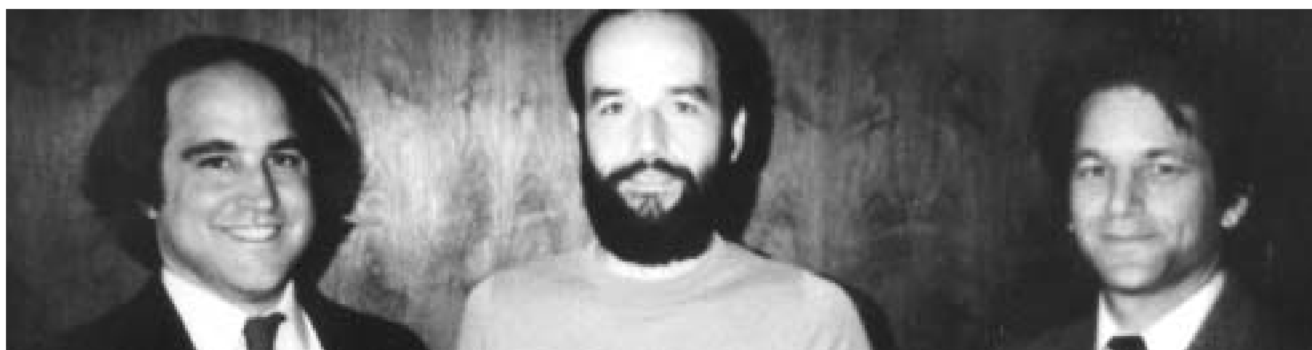
Het vinden van getallen x en y is het kernprobleem en met name het *uitsluiten* van mogelijke waarden van x en y is intensief bestudeerd. In de NFS- en QS- methode worden x^2 en y^2 geconstrueerd door relaties te verzamelen. Een relatie is voor te stellen door een getallenpaar (a, b) zodat 77 een deler is van het verschil $a - b$. Verder moeten zowel a als b alleen 'kleine' priemfactoren bevatten. Wanneer we met 'klein' bedoelen niet groter dan 5, dan is $(50, -27)$ een relatie want: $50 - (-27) = 77$, $50 = 2 \times 5^2$ en $-27 = (-1) \times 3^3$.

Enkele relaties:

relatie (a, b)	ontbinding van a	ontbinding van b
(45, –32)	$3^2 \times 5$	$(-1) \times 2^5$
(50, –27)	2×5^2	$(-1) \times 3^3$
(80, 3)	$2^4 \times 5$	3
(125, 48)	5^3	$2^4 \times 3$
(320, 243)	$2^6 \times 5$	3^5

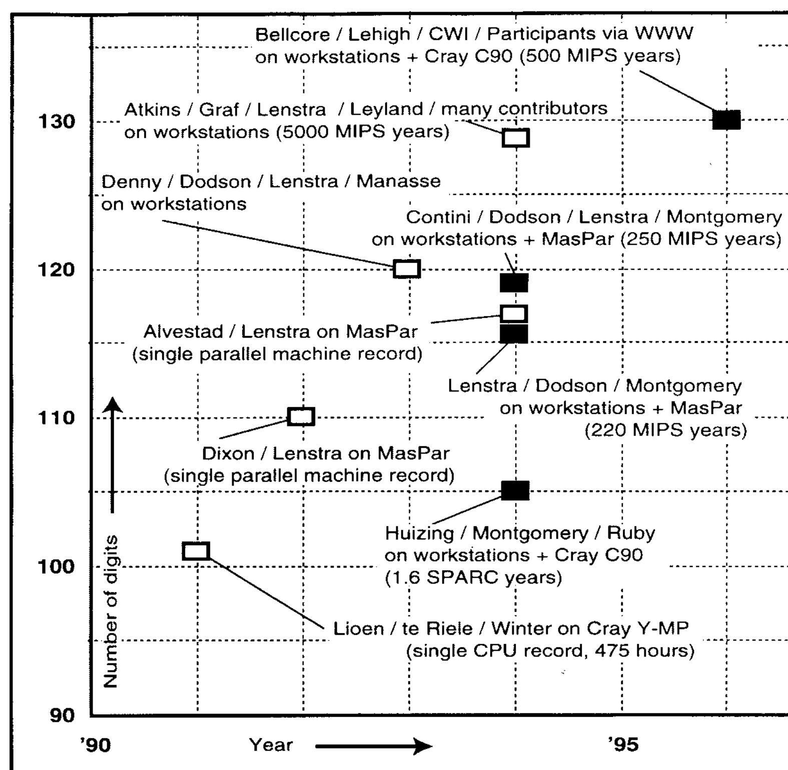
Het zeefproces bestaat uit het op zeer efficiënte wijze verzamelen van relaties. Wanneer er voldoende relaties verzameld zijn (deze fase kost verreweg de meeste rekentijd) wordt een selectie gemaakt zó dat zowel de gekozen a's als de gekozen b's met elkaar vermenigvuldigd een kwadraat zijn. Kiezen we bijvoorbeeld (80, 3) en (320, 243) dan is $80 \times 320 = 2^{10} \times 5^2 = 160^2$ een kwadraat, evenals $3 \times 243 = 3^6 = 27^2$. Bovendien geldt dat 77 een deler is van het verschil van de kwadraten. Zo'n paar kwadraten heeft een kans van minstens een half om 77 in factoren te ontbinden. Het maken van een selectie gebeurt in de voorlaatste fase en vergt voor grote getallen tijdrovende operaties op een zeer grote matrix gevuld met nullen en enen. In de NFS bestaan de relaties, in tegenstelling tot in de QS, niet uit gewone getallen, maar uit 'algebraïsche' getallen. Een voorbeeld van zo'n getal is $a + b\sqrt{2}$, waarbij a en b gehele getallen zijn. Ook bij algebraïsche getallen kunnen we spreken van zuivere kwadraten: zo is $3 + 2\sqrt{2}$ het kwadraat van $1+\sqrt{2}$. Na het maken van een selectie hebben we twee kwadraten van algebraïsche getallen gevonden. Uit deze kwadraten x^2 en y^2 worden in de laatste fase de wortels getrokken en wordt op de gebruikelijke manier een factor gezocht door middel van het berekenen van een grootste gemeenschappelijke deler.

een 100 Mhz Pentium processor zou met deze methode zo'n 18 jaar nodig hebben gehad voor het kraken van RSA-130. Toch nog tien keer zo snel als de oudere Quadratic Sieve methode, waarmee in 1994 het vorige wereldrecord van 129 cijfers werd gevestigd. (Rivest daagde in 1977 de wereld uit dit getal te kraken en schatte dat dat met de toenmalige middelen 10^{15} jaar zou duren! Zeventien jaar later



De uitvinders van het RSA-Cryptosysteem: van links naar rechts R.L. Rivest, A. Shamir, L. Adleman. *Foto: RSA Data Security Inc.*

nam dit acht maanden in een wereldwijde samenwerking.) Werd de benodigde rekentijd voorheen voornamelijk gevonden op enkele grote onderzoekinstituten die met het project meededen (zoals het CWI), vanaf december 1995 kan iedereen met een werkstation en een Internet-verbinding een bijdrage leveren door het verzamelen van relaties (zie kader). Op deze manier fungeert Internet als de grootste parallelle supercomputer ter wereld (zie ook: http:////www.npac.syr.edu/factoring.html). De Nederlandse wiskundige Arjen Lenstra (Bellcore, V.S.) initiëerde dit project. World Wide Web pagina's geven informatie, aanmeldingsformulieren en aanwijzingen over de installatie van zijn programma. Deelnemers worden automatisch van taken voorzien en de gevonden relaties worden automatisch naar een verzamelpunt verzonden. Een grote partner is het CWI, waar mevr. Elkenbracht-Huizing zo'n 20 miljoen van de benodigde 70 miljoen relaties verzamelde. Zij had daarbij de beschikking over de ongebruikte rekentijd 's nachts en in het weekeinde van 60 werkstations.



Factoriseringsrecords in de jaren negentig, met de Quadratic Sieve ☐ en de Number Field Sieve ■

Na de fase van verzamelen zijn de laatste twee fasen op het CWI uitgevoerd. Voor de ontbinding van getallen van meer dan 110 cijfers zou de Number Field Sieve (NFS) sneller moeten zijn dan de oudere Quadratic Sieve. Bij de uitvoering rezen er echter nog problemen met de NFS methode. Allereerst moesten er bewerkingen op een gigantische matrix zeer snel kunnen worden uitgevoerd, waarvoor nog geen methode voorhanden was. En in de laatste fase van de NFS methode moest nog de wortel worden getrokken uit een groot 'algebraïsch' getal (zie kader). Voor beide problemen bedacht de Amerikaan Peter Montgomery tijdens een gastverblijf op het CWI een nieuwe aanpak. Met de daaruit resulterende computerprogramma's kon tenslotte de NFS met succes worden toegepast op de ontbinding van RSA-130. Hierbij was de Cray C90 supercomputer van het Amsterdamse rekencentrum SARA vanwege zijn zeer grote geheugen een onontbeerlijk hulpmiddel. (WIN96/1)

Noot

1 Het CWI is een nationaal instituut voor onderzoek in de wiskunde en de informatica. Er werken ca. 150 onderzoekers. De nadruk ligt op grensverleggend onderzoek voor praktische vraagstukken en de overdracht van nieuwe kennis naar de maatschappij. Het instituut onderhoudt een breed scala aan contacten met universiteiten, industrieën, grote technologische instituten, en particuliere en overheidsinstellingen. Het CWI is een der oprichters van ERCIM, het European Research Consortium for Informatics and Mathematics.

EUCLIDES

Inhoud van de 71e jaargang 1995/1996

Verenigingsnieuws

Nederlandse
Vereniging van
Wiskundeleraren

Van de bestuurstafel

Regionale bijeenkomsten

De voorbereidingen op de **regionale bijeenkomsten** zijn alweer in volle gang. Dit jaar zijn drie bijeenkomsten gepland:
11, 13 en 18 maart in resp. *Zwolle, Leiden en Eindhoven*.
Houdt alvast een plaatsje vrij in uw agenda!
We zouden graag de leuze ‘voor leden, door leden’ meer inhoud willen geven door ruimte te bieden aan gewone leden om een bijdrage te leveren tijdens deze bijeenkomsten.

Tweede fase havo/vwo

Er wordt op veel plaatsen hard gewerkt aan de voorbereiding op de nieuwe programma’s. Het PROFI-project is op de experimenteerscholen het examenjaar ingegaan. Daarnaast is een aantal gewone scholen in samenwerking met APS/Fi dit jaar begonnen met een experiment in de vierde klas vwo. Hiermee wordt enigszins tegemoet gekomen aan het bezwaar dat we al eerder naar voren brachten, namelijk dat voor een helder beeld de experimenten niet alleen zouden moeten plaatsvinden in een ‘koesteromgeving’ met veel begeleiding en extra faciliteiten. De echte invoering van het nieuwe programma zal uiteindelijk ook op gewone scholen gestalte moeten krijgen.

SLO-project informatietechnologie

De gezamenlijke aanvraag van I&I en de NVvW is toegewezen. Het project zal in januari 1997 van start gaan. Hier onder volgt de tekst van de aanvraag.

De Nederlandse Vereniging van Wiskundeleraren (NVvW), daarbij ondersteund door de vereniging voor informatiekunde en informatietechnologie in onderwijs (I&I) zou het op prijs stellen als de SLO nadere inspanningen zou willen verrichten op het terrein van het onderzoeken van de mogelijkheden tot ***zinvolle en verantwoorde toepassing*** *van informatietechnologie (IT) in het wiskundeonderwijs, met name gericht op inpassen in het curriculum in de vernieuwde tweede fase havo/vwo.*
Toelichting:
In de plannen van de vakontwikkelgroep wiskunde is een grote rol weggelegd voor het gebruik van IT. De grafische rekenmachine wordt verplicht voor iedereen en voor de computer is plaats ingeruimd bij verkenning en onderzoek, maar ook als gereedschap of als studiehulp. Uit het rapport van de studiecommissie wiskunde B vwo blijkt dat eind 1993 de computer nog maar op zeer beperkte schaal werd ingezet. Er zijn geen aanwijzingen dat die situatie inmiddels drastisch veranderd is. Redenen daarvoor zijn o.a. behalve praktische belemmeringen als beschikbaarheid van hardware ook gelegen in kwaliteit en bruikbaarheid van de beschikbare software, waardoor het gebruik ervan geen meerwaarde oplevert. Hier gaapt een kloof.
Wil die situatie in 1998 bij het invoeren van de nieuwe programma’s veranderen dan zal op z’n minst de meerwaarde van het gebruik van IT duidelijk moeten worden. Dat vereist een nauwkeurige en nuchtere doordenking van de didactische en wiskundige aspecten van het gebruik van IT in het nieuwe wiskundeprogramma in zijn geheel, naast uiteraard het ontwikkelen van bijpassende software. Immers de aktiviteiten die tot nu toe zijn ontwikkeld, hadden betrekking op onderdelen, het niveau van ‘pakketjes’. De valkuilen zijn velerlei: Een te vroeg of verkeerd inzetten van de computer kan het begrip eerder verduisteren dan verhelderen, handelen en begrijpen kunnen makkelijk ontkoppeld worden.
Verschillen tussen leerlingen, in het bijzonder tussen meisjes en jongens, kunnen door een bepaalde aanpak eerder vergroot dan verkleind worden.
Wensen m.b.t. de uitvoering.
Gezien het bovenstaande is het van belang dat niet door een groep van louter ‘gelovigen’ over deze zaken wordt nagedacht, en dat waar mogelijk gebruik wordt gemaakt van expertise op het terrein van vrouwen/meisjes en informatica.

Het bestuur van NVvW en I&I.

OPROEP

Het bestuur is op zoek naar mensen die zitting willen nemen in de resonansgroep bij dit project, teneinde de gang van zaken te volgen en van commentaar te voorzien. Als u zelf belangstelling hebt, danwel de aandacht wilt vestigen op anderen die u deskundig acht, stuurt u dan even een briefje naar

M. Kollenveld
Leeuwendaallaan 43
2281 GK Rijswijk.

Marian Kollenveld

Internet en digitale school

Steeds meer wiskundedocenten oriënteren zich op Internet. Op Internet zijn allerlei zaken te vinden die voor wiskundedocenten van belang kunnen zijn.
Zo is er bijvoorbeeld een Digitale School met daarin een Digitaal Wiskundelokaal.
Ook veel scholen hebben tegenwoordig pagina's op het World Wide Web (WWW) over wiskundeonderwijs. Zoals bijvoorbeeld SG De Grundel uit Hengelo, Notre Dame des Anges uit Ubbergen, het Spinoza Lyceum uit Amsterdam en het St. Michael College uit Zaandam. Aan deze laatste school ben ik verbonden als wiskundedocent. Tevens doe ik het beheer van het Digitale Wiskundelokaal.

Gerard Koolstra

Hieronder volgen een aantal adressen:
http://digischool.bart.nl/wi/wilok.htm
http://home.pi.net/~Grundel/alfwi.html
http://www.telebyte.nl/Notredame/Project.htm
http://www.xs4all.nl/~Spinoza/vakken/wiskunde/wiskunde.html
http://www.xs4all.nl/~gerardk/smcwi.html

Ook in de kalender achterin dit nummer staan mogelijke interessante 'sites'.

Verschenen

De redactie van Euclides ontving van een tweetal boeken een nieuwe druk. Het betreft in beide gevallen boeken die reeds eerder in Euclides besproken werden, en bovendien zijn er slechts kleine verschillen met de vorige druk. In de meeste gevallen gaat het alleen om wat verbeteringen. We vermelden daarom deze boeken kort, en verwijzen naar de eerdere uitvoeriger besprekingen.

A. van Rooij
Analyse voor beginners

Uitg. Epsilon, Utrecht (1996)
f 42,50; 276 bladzijden
ISBN 90-5041-005-7

Dit is grotendeels de tekst van een syllabus die gebruikt werd in Nijmegen bij het onderwijs in de analyse aan eerstejaars wiskunde-studenten. Dit boek werd eerder besproken in Euclides, 63e jaargang.

R.A. Kortram
De theorie van complexe functies

Uitg. Epsilon, Utrecht (1996)
f 37,50; 176 bladzijden
ISBN 90-5041-017-0

Ook dit is een bewerking van een syllabus uit Nijmegen; het boek sluit min of meer aan bij het vorige. Dit boek werd besproken in Euclides, 66e jaargang.



S.P. van 't Riet
Het didactisch handelen van wiskundedocenten met betrekking tot interne differentiatie

Op 10 april 1995 is *Peter van 't Riet* aan de Vrije Universiteit te Amsterdam gepromoveerd op het in de titel genoemde proefschrift. Het onderzoek waarvan het proefschrift verslag doet, is voortgekomen uit een aantal projecten rond het thema 'de professionele ontwikkeling van docenten in het voortgezet onderwijs', meer in het bijzonder het thema 'didactische differentiatie'. De directe aanleiding was dat de onderzoeker als opleider van aanstaande wiskundeleraren geïnteresseerd is in de voorkomende vormen van differentiatie in didactisch handelen bij wiskundedocenten en de daarbij relevante factoren. En dan gaat het om factoren als de mate van differentiatie in het gebruikte leerboek en de wijze waarop de leerlingengroep is samengesteld. Vervolgens hoe een en ander het beste aan aankomende wiskundeleraren onderwezen zou kunnen worden.
In het boek wordt interne-differentiatiegedrag van wiskundedocenten gedefinieerd als dat didactisch handelen van docenten tijdens de voorbereiding, uitvoering en evaluatie van in klasseverband georganiseerde lessen, dat op basis van individuele verschillen leidt tot een verschillende behandeling van leerlingen of groepjes leerlingen ten aanzien van het totale onderwijsleerproces, de leeractiviteiten, de onderwijsinteracties en/of de leerprocesevaluatie. Het feitelijke onderzoek heeft zich beperkt tot het aspect uitvoering. Het interne-differentiatiegedrag is vervolgens in drie categorieën ingedeeld. *Van 't Riet* onderscheidt productgeoriënteerd interne-differentiatiegedrag: leerlingen worden benaderd in termen van zwakke en goede leerlingen, meestal gebaseerd op een algemene indruk die een leraar heeft en procesgeoriënteerd interne-differentiatiegedrag: op grond van spontaan optredende verschillen in bijvoorbeeld aanpak of behoefte aan hulp worden leerlingen of groepjes verschillend benaderd. Daarnaast is er het gedrag waarbij de leerkracht alle leerlingen uniform benadert: non-differentiatiegedrag.
Ook bij de twee grote wiskundemethoden is een dergelijke indeling te maken. *Van 't Riet* beargumenteert dat Moderne Wiskunde vooral een procesgeoriënteerde methode is en Getal en Ruimte een meer productgeoriënteerde.

Het onderzoek is uitgevoerd in brugklassen mavo/havo/vwo, die of heterogeen (mhv) of naar niveau (mh en hv) waren ingedeeld. De methode van onderzoek bestond vooral uit het voorleggen van een vragenlijst aan de docenten waarin zij

Wintersymposium 1997

Het Wintersymposium van het Wiskundig Genootschap zal in 1997 plaatsvinden op 4 januari en wordt gehouden in het *Johan van Oldenbarnevelt Gymnasium, Thorbeckeplein 1, Amersfoort.*
Het symposium is in de eerste plaats bedoeld voor leraren, maar natuurlijk is iedere belangstellende van harte welkom. Het symposium is dit keer gewijd aan de **geschiedenis van de wiskunde**. Aan de orde komen o.a. de vergelijking van de derde graad, de historie van de differentiaalrekening en het wiskundig werk van de broers Jakob en Johann Bernoulli. Waarbij aandacht voor de harmonische reeks en de snelste glijbaan.

	PROGRAMMA
09.30-10.00	Ontvangst met koffie
10.00-11.00	**Rondom de vergelijking van de derde graad** Prof.dr. A.W. Grootendorst
11.00-11.15	pauze, met koffie
11.15-12.15	**Differentiaalrekening: verleden, heden en toekomst** Prof.dr. H.J.A. Duparc
12.15-13.30	pauze, waarin men kan deelnemen aan een gezamenlijke lunch.
13.30-14.30	**De 'Bernoulli Brothers' in de wiskundige arena rond 1697** Dr. J.A. van Maanen

De deelname is *GRATIS*.

Wie wil meedoen aan de gezamenlijke lunch wordt verzocht *voor 31 december 1996 f* 17,50 over te maken op gironummer *3391318* van *R. Bosch, Heiakker 16* in *Prinsenbeek*.
Wie in aanmerking wil komen voor een certificaat vermeldt bij betaling: Certificaat.
Indien u niet wilt deelnemen aan de lunch maar wel een certificaat wenst, stuurt u een briefje met dit verzoek naar bovengenoemd adres.

Voor inlichtingen kunt u bellen naar
076-5273267 (overdag) of 076-5419757 ('s avonds).

---

zichzelf moesten beoordelen op de genoemde vormen van interne-differentiatiegedrag. Vrijwel dezelfde vragenlijst werd ook aan hun leerlingen voorgelegd: zij moesten hun docent op dit punt beoordelen. Door middel van deze vragenlijsten en door te kijken naar de gebruikte wiskundemethoden werden de volgende hypothesen getoetst.
(1) De mate waarin een wiskundemethode de nadruk legt op een bepaalde interne-differentiatiemethodiek, heeft een positieve invloed op de mate waarin de docenten overeenkomstig die methodiek handelen.
(2) Wiskundedocenten die lesgeven in heterogene lesgroepen vertonen meer interne-differentiatiegedrag dan wiskundedocenten die lesgeven in homogene lesgroepen.
De resultaten zijn als volgt weer te geven. Het onderzoek bevestigt dat er inderdaad twee vormen van interne-differentiatiemethodieken zijn: de proces- en de productgeoriënteerde, welke hun doorwerking hebben in zowel de leerstof van wiskundemethoden als in het interne-differentiatiegedrag van docenten. De in een wiskundemethode gerealiseerde methodiek heeft invloed op de mate waarin docenten overeenkomstig die methodiek handelen. Voor de procesgerichte interne-differentiatiemethodiek was de invloed significant, voor de productgerichte niet. De toepassing van de heterogene of homogene groeperingsvorm heeft echter geen duidelijke invloed op het interne-differentiatiegedrag. Verder is het opmerkelijk dat de leerlingen minder interne-differentiatiegedrag waarnemen dan hun docenten. Hierbij is het de vraag wie dat het best kan beoordelen: de leraar zelf of de leerling. Hij heeft gevonden dat het percentage meisjes een positieve invloed heeft op het procesgeoriënteerde interne-differentiatiegedrag van wiskundedocenten.
De auteur vermeldt tot slot dat er een opleidingsplan voor aanstaande docenten is te ontwerpen waarin relevante beroepsvereisten en -bekwaamheden ten aanzien van interne differentiatie aan de orde kunnen komen, maar concrete suggesties heb ik niet gevonden. Ditzelfde geldt voor zijn 'claim' dat het onderzoek aanknopingspunten biedt voor wiskundedocenten, - secties, auteurs en uitgevers van wiskundemethoden om tot verbetering te komen van de kwaliteit van interne differentiatie in het wiskundeonderwijs.

Het proefschrift overziende, bekruipt mij wat onvrede. Ik had graag meer aandacht gezien voor de relatie tussen interne differentiatie en de kwaliteit van het onderwijs. Je mag toch aannemen dat interne differentiatie op de een of andere manier en in een of ander opzicht leidt tot beter wiskundeonderwijs. In de theoretische onderbouwing wordt daar wel het een ander over gezegd, maar bij het feitelijk onderzoek en de conclusies zie ik het nauwelijks terug. Een dergelijk wiskundig-didactisch onderzoek wint voor mij aan waarde, als de wiskundedocent in de klas er in concrete zin zijn voordeel mee kan doen. Dat eventuele voordeel is voor mij onduidelijk gebleven.

Bert Zwaneveld

Wintersymposium 96 belicht coderingstheorie en cryptologie

Veilig communiceren

E.M. van de Vrie

Op 6 januari 1996 vond het traditionele wintersymposium plaats van het Wiskundig Genootschap. Wederom was de locatie het Johan van Oldenbarnevelt Gymnasium in Amersfoort. Op deze winterse dag waren bijna tweehonderd geïnteresseerden,voornamelijk leraren uit het voortgezet onderwijs, uit heel Nederland afgereisd om geïnformeerd te worden over onderwerpen uit de coderingstheorie en de cryptologie. Deze onderwerpen uit de discrete wiskunde worden steeds belangrijker, nu er steeds massaler gebruik gemaakt wordt van elektronische communicatie en betalingen. De wiskundige basis van deze onderwerpen ligt in de abstracte algebra, en dan vooral in de theorie van de eindige lichamen, maar veel toepassingen zijn ook zonder diepgravende wiskunde te volgen. Sterker nog, heel wat onderwerpen die aan bod kwamen, zijn in de klas te behandelen en laten dan een heel andere kant van de wiskunde zien dan we gewend zijn.

Fouten maken en herstellen

Drs. M. van der Vlugt van de Universiteit Leiden introduceerde de coderingstheorie aan de hand van de Hamming-code. Als er een rij nullen of enen elektronisch verstuurd moet worden, dan kunnen daar fouten in ontstaan, zodat een andere rij wordt ontvangen dan was verstuurd. Als dat het rekeningnummer was waarnaar iemands salaris moest worden overgemaakt, is dat natuurlijk knap vervelend. Om fouten op te sporen, of eventueel te herstellen, wordt daarom een rij nullen en enen in korte stukjes geknipt en aan ieder stukje wordt op een slimme manier een aantal extra enen en nullen toegevoegd. Welke nullen en enen moeten worden toegevoegd en hoe geconstateerd kan worden waar er welke fouten zijn opgetreden, dat is het onderwerp van de coderingstheorie. Bij een Hamming-code worden de nullen en enen die moeten worden toegevoegd, bepaald door sommige van de nullen en enen van het oorspronkelijke stukje bij elkaar op te tellen. Er kunnen dan alleen maar bepaalde nieuwe rijtjes ontstaan. Wordt een rijtje ontvangen dat niet gemaakt had kunnen worden, dan is blijkbaar een fout opgetreden, en die is soms weer te herstellen. Hamming-codes zijn relatief eenvoudig, maar hebben ook hun beperkingen. In vele toepassingen zijn geavanceerdere codes noodzakelijk. Van de Vlugt behandelde een aantal aspecten die daarbij een rol speelden.





Geheime berichten en ware handtekeningen

Naast het voorkomen van fouten die bij elektronische communicatie op kunnen treden, is het soms van groot belang dat onbevoegden niet een bericht kunnen lezen of anderszins misbruiken. Nu er zeer veel betalingsopdrachten via telefoonlijnen verstuurd worden, is het bijvoorbeeld zeer ongewenst dat iemand het bericht dat een opdracht voor een salarisbetaling is, af kan luisteren en een aantal malen kan herhalen. Anderzijds is het van belang dat de ontvanger van een belangrijke boodschap zeker weet dat de afzender degene is wiens naam onder het bericht staat en niet misleid wordt door iemand met minder fraaie bedoelingen.
Prof. H. van Tilborg van de Technische Universiteit Eindhoven schetste hoe in de cryptologie vele technieken zijn ontwikkeld om deze problemen op te lossen, waarvan de geschiedenis terug gaat tot de Romeinse tijd. Julius Ceasar verving bijvoorbeeld de letters in een bericht door letters die in het alfabet een vast aantal plaatsen verder staan. Zo'n systeem is echter makkelijk te ontcijferen: maximaal 26 keer proberen hoeveel letters je terug moet gaan om een leesbaar bericht te krijgen. De ontwikkelingen in de cryptologie zijn er voor een groot deel op gericht geweest om methoden te vinden waarbij het heel gemakkelijk is om een bericht te vercijferen (om te zetten in een geheimschrift), maar heel moeilijk om het te ontcijferen. Ter illustratie gebruikte Van Tilborg daar het Engels-Poolse woordenboek voor: het Poolse woord dat bij een zeker Engels woord hoort, is daarin makkelijk te vinden, maar als bij dat Poolse woord het oorspronkelijke Engelse woord moet worden teruggevonden, is het een bijna onmogelijke opgave (tenzij je

natuurlijke het Pools-Engels woordenboek hebt). Van een soortgelijk principe maken ook moderne publieke-sleutelsystemen gebruik. Daarin wordt openbaar gemaakt hoe je een bericht moet vercijferen (vergelijk het gebruik van het woordenboek Engels-Pools), maar het ontcijfermechanisme (het woordenboek Pools-Engels) wordt geheim gehouden. Iedere gebruiker in dat systeem kan als het ware een eigen set woordenboeken maken. Als een gebruiker maar een van de woordenboeken openbaar maakt, kunnen anderen veilig berichten sturen die ze met dat woordenboek hebben vercijferd, want de oorspronkelijke gebruiker is immers de enige die ze kan ontcijferen met het andere woordenboek, dat dan wel zorgvuldig geheim moet worden gehouden. De constructie met van die woordenboeken is gebaseerd op stellingen van Euler en Fermat, die waarschijnlijk nooit zouden hebben kunnen bevroeden hoe hun geestesprodukten nog eens toegepast zouden kunnen worden. In deze constructies wordt volop gebruik gemaakt van (grote) priemgetallen. Bijna dezelfde methoden kunnen worden gebruikt om handtekeningen onder berichten te zetten, die daarna niet meer door de verzender kunnen worden ontkend.

Elektronische bankbiljetten

Elektronische betalingen spelen een steeds belangrijkere rol in onze samenleving. Op dit moment moet daarbij veelal even contact gelegd worden (op een veilige manier) met een centrale computer, om geld over te schrijven van de ene op de andere bankrekening. Daarmee is dan een betaling verricht. Maar in die centrale computer worden op die manier wel erg veel gegevens opgeslagen, waarvan we als burgers misschien willen dat dat niet het geval zou zijn. Want het is misschien niet zo heel erg als ergens is vastgelegd dat er op een bepaalde plaats, op een bepaald tijdstip een bepaald bedrag van de ene bepaalde persoon naar de andere bepaalde persoon is overgegaan, maar het - Big brother is watching you - gevoel dringt zich daarbij wel erg snel op. Prof. J. van de Craats van de Universiteit van Amsterdam en de Open universiteit vertelde dat ook systemen zoals de chipknip dit probleem niet oplossen, en dat daarom verder wordt gezocht naar elektronische systemen die even anoniem kunnen functioneren als de aloude munten en bankbiljetten. Belangrijke stappen daarin zijn gezet door het Amsterdamse bedrijf ‘Digicash’ van David Chaum. Unieke (zeer grote) getallen functioneren daarbij als bankbiljetten. Deze getallen zijn zelf geen priemgetallen, maar bij het fabriceren ervan worden wel grote priemgetallen gebruikt. De getallen worden uitgegeven door een centrale bank en vertegenwoordigen dan een geldswaarde. Iemand die wat koopt, geeft het getal door aan de verkoper en verricht daarmee de betaling. Als de verkoper het getal bij de bank inlevert, wordt het betreffende bedrag op de rekening bijgeschreven. Een dergelijk systeem blijkt te kunnen functioneren en aan veel van de privacy-eisen te kunnen voldoen. Natuurlijk moet er wel voor het nodige gezorgd worden: iemand moet niet in staat zijn om twee keer met hetzelfde getal te betalen, een ontvanger van een getal moet zeker weten dat het weer kan worden ingewisseld bij de bank, enzovoorts, maar voor al die problemen blijken oplossingen te bestaan. Wellicht dat dit soort systemen de opvolgers worden van de chipknip-systemen die momenteel ingevoerd worden. De snelle ontwikkelingen in de chip-technologie zullen dat zeker mogelijk maken.

Literatuur

Er is heel wat literatuur over coderingstheorie en cryptologie. In boekhandels en bibliotheken is daar het nodige over te vinden. Op het wintersymposium lieten uitgeverij Epsilon en de Open universiteit zien wat ze op dit terrein, maar ook over andere wiskundeonderwerpen, te bieden hebben. Deze organisaties kunnen u daar desgewenst verder over informeren.

Epsilon

Prof. F. Verhulst
Universiteit Utrecht
Postbus 80010
3508 TA Utrecht
tel. 030-2531526
e-mail: verhulst@math.ruu.nl

Open universiteit

Ir. E.M. van de Vrie
Postbus 2960
6401 DL Heerlen
tel. 045-5762366
e-mail: evert.vandevrie@ouh.nl.

Op de jaarvergadering 1993 van de NVvW werd besloten een fonds in het leven te roepen om het wiskundeonderwijs in de Derde Wereld te ondersteunen door financiële bijdragen aan een nader te bepalen project. Een tweede minstens zo belangrijk doel was wiskundedocenten 'hier' te laten zien dat er 'daar' ook collega's zijn die zich met soortgelijke vragen en problemen bezig houden als zij. Dat wiskundeonderwijs niet ophoudt bij de grenzen van Nederland of de westerse wereld. Het volgende artikel is het derde en laatste uit een serie ontdekkingsreizen naar dat onderwijs 'daar'.

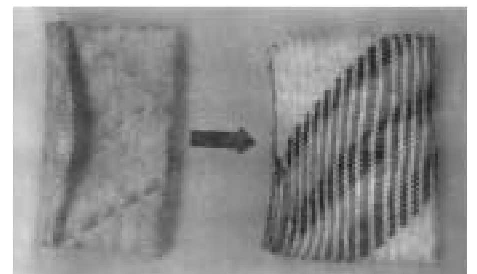
Wiskunde-onderwijs in de Derde Wereld (deel 3)

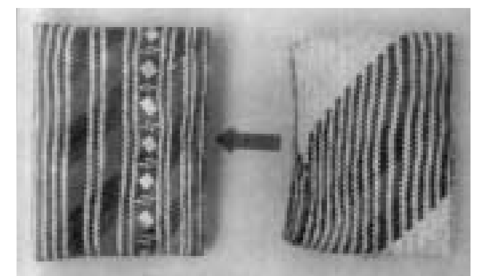
Hans Wisbrun

Iedere cultuur bouwt wiskunde, dat is kort samengevat het uitgangspunt van de stroming binnen de wiskundedidactiek die met Etnomathematica wordt aangeduid. Het onderwijs binnen een bepaalde cultuurgroep zou (mede) gebruik moeten maken van de eigen ontstaansgeschiedenis van de wiskunde. Met name in Derde Wereldlanden kan deze benadering een interessant alternatief bieden voor de manier waarop de wiskunde daar doorgaans wordt onderwezen, namelijk als import-artikel uit de westerse wereld. In dit artikel wordt, bij wijze van voorbeeld, een concrete uitwerking van dit idee gegeven, zoals beschreven door Paulus Gerdes en Gildo Bulafo [1]). Dat dit voorbeeld uit Moçambique komt is niet toevallig, omdat ik daar zelf enige jaren gewerkt heb. Op het einde van dit artikel komt nog een kritische discussie naar aanleiding van het beschreven voorbeeld en een terugblik op de hele serie artikelen over wiskundeonderwijs in de Derde Wereld.

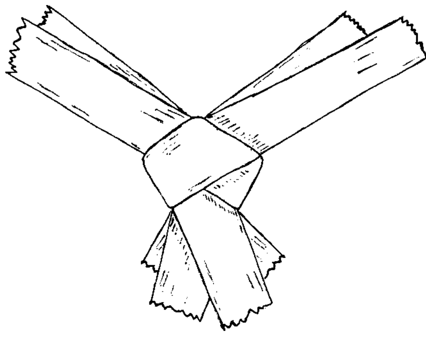
Sipatsi

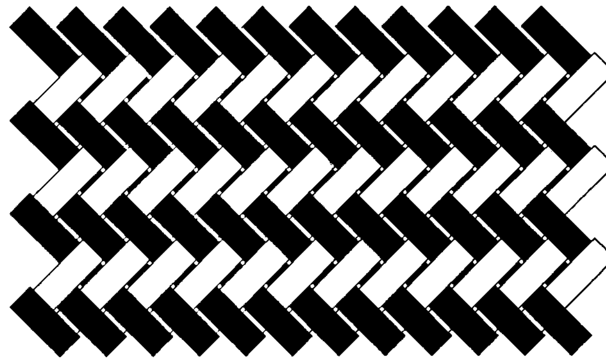
Sipatsi (enkelvoud: gipatsi) zijn gevlochten portefeuilles, zoals die in een bepaalde provincie van Moçambique, Inhambane, worden gemaakt. Ze worden gebruikt voor het bewaren en meenemen van munten en persoonlijke documenten. Een gipatsi bestaat uit drie delen die in elkaar passen:



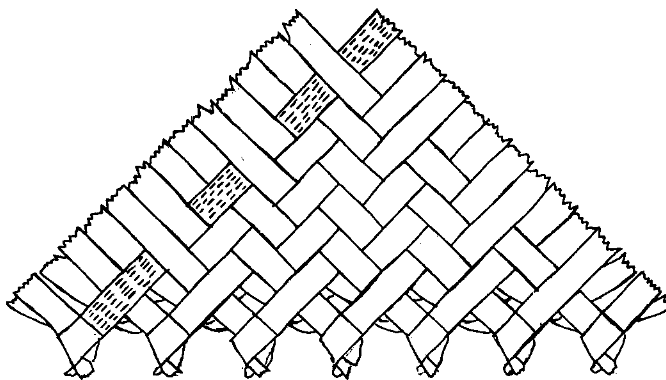


Sipatsi worden gevlochten uit het blad van een bepaald type palmboom. Dat blad wordt eerst met een soort naald in strengen van gelijke breedte verdeeld. Het vlechtwerk begint met het maken van knopen

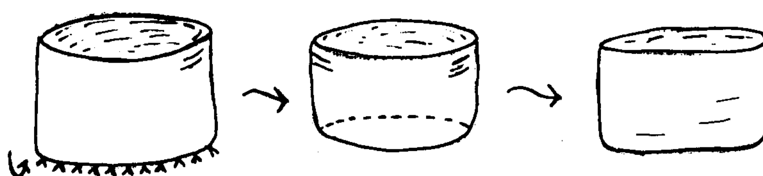

afbeelding 2


afbeelding 5

In iedere knoop komen twee paar strengen samen. Vervolgens worden de knopen aan elkaar verbonden door de uiteinden aan de bovenkant met elkaar te vervlechten, meestal volgens het principe 'twee erboven, twee eronder'. De strengen aan de onderkant van de knopen worden er afgeknipt:


afbeelding 3

Op deze manier onstaat een soort matje. Nu wordt een tweede matje gemaakt, met hetzelfde aantal knopen. Het tweede matje wordt een halve slag gedraaid en de uitstekende strengen van beide matjes worden met elkaar verweven en zo onstaat een cilinder. Dan worden de knopen naar binnen gevouwen en wordt de cilinder geplet:


afbeelding 4

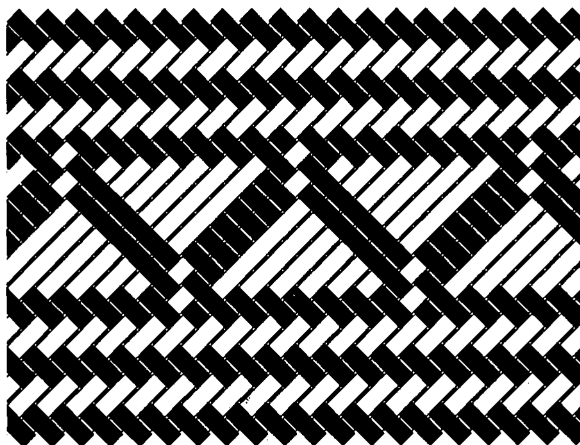
De onderkant wordt nu vastgenaaid en de bovenkant afgezoomd. Een gipatsi bestaat uit drie van deze geplette cilinders, die iets verschillen in maat en daardoor in elkaar passen.
Door bij de knopen strengen van verschillende kleuren te gebruiken kunnen sipatsi versierd worden. We noemen het ene paar strengen wit (in feite: de natuurlijke kleur van de strengen) en het andere paar zwart (in feite: groen, paars, donkerblauw, enzovoort). De witte strengen maken een hoek van 45° met de onderkant, de zwarte een hoek van 135°. In de meest eenvoudige vorm ontstaat zo een patroon als in afbeelding 5.

Door variaties in het vlechtpatroon kunnen allerlei verschillende decoratiestroken gemaakt worden. Afbeelding 6 is een voorbeeld.

Waar zit nu de wiskunde van deze sipatsi? Wat voor mogelijkheden biedt deze traditionele ambachtelijke techniek voor het wiskundeonderwijs in Moçambique? Het zal de lezer van dit blad al duidelijk zijn, dat er bijvoorbeeld rekenkunde verborgen zit in de vervaardiging van sipatsi. Zo is er een verband tussen het aantal knopen van een gipatsi en de verschillende decoratiestroken die mogelijk zijn. Ik denk niet dat de sipatsi-makers dat verband zelf zouden kunnen verwoorden, maar de praktijk van het vlechten zal hen zeker een aantal ervaringsregels hebben geleerd. Leerlingen nemen die regels van huis mee als zij naar school gaan en dat zou een aanknopingspunt voor wiskundeonderwijs kunnen zijn.
Hieronder volgt een uitwerking van dit idee, zoals door Paulus Gerdes gebruikt wordt op de universitaire lerarenopleiding in Maputo. Er staan vragen bij, dus u wordt bij deze ook zelf uitgedaagd.

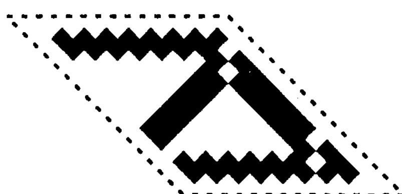
Sipatsi en rekenen

Een decoratiestrook [2]) van een gipatsi bestaat uit een motief dat een aantal malen herhaald wordt. In afbeelding 7 staat zo'n strook, met het daarbij behorende motief.



afbeelding 6

Voor de duidelijkheid zijn nu geen individuele strengen meer getekend.





afbeelding 7

De strook loopt aan beide kanten van de gipatsi. Wiskundig uitgedrukt: op papier loopt de strook oneindig ver naar links en naar rechts door.
Je kunt zeggen dat elk motief een *periode* heeft. Zo heeft het hierboven getekende motief een periode 8. Die 8 is ook het aantal gekleurde strengen dat nodig is om het betreffende motief te maken.
Als een motief met periode p een geheel aantal keren op een gipatsi past, dan betekent dat, dat tevens het totaal aantal gekleurde strengen van die gipatsi, T, een veelvoud van p is. Bovendien moet het totaal aantal gekleurde strengen T een veelvoud van 4 zijn: uit iedere knoop komen twee gekleurde strengen en het aantal knopen is altijd even (omdat een gipatsi bestaat uit twee gelijke kanten).
Dus T moet een veelvoud van p èn van 4 zijn. Bij een periode van bijvoorbeeld 9, betekent dat, dat T een veelvoud van 36 is. Als er verschillende motieven met verschillende perioden, p_i, gebruikt worden, dan moet T een veelvoud zijn van alle p_i èn van 4. Als dat niet het geval is, dan zitten er onregelmatigheden in het patroon en dat wordt als gebrek aan kwaliteit gezien.
Vragen die naar aanleiding hiervan gesteld kunnen worden zijn:
- Sipatsi-makers gebruiken vaak 24 knopen voor elke kant van een gipatsi. Kun je een reden bedenken voor die keuze?
- Op sipatsi komen vaak motieven voor met een periode 8. Wat betekent die keuze voor het aantal knopen aan iedere kant van een gipatsi?
- Bekijk het onderstaande gedeelte van een gipatsi (afbeelding 8). Wat kun je zeggen over het totale aantal knopen dat voor de hele gipatsi nodig is?



afbeelding 8

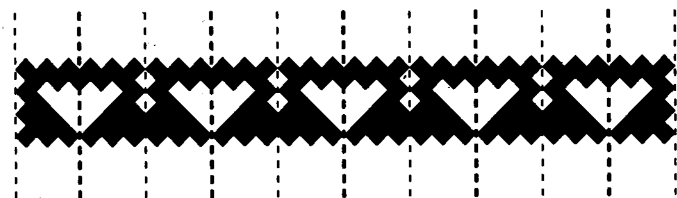
Sipatsi en symmetrie

In gipatsi-patronen zijn allerlei vormen van symmetrie te onderscheiden. Op de volgende pagina staan drie voorbeelden.

Dit geeft aanleiding tot vragen als:
- Een patroon heeft zowel horizontale als verticale spiegelsymmetrie. Moet het dan ook (180°-) draaisymmetrie hebben?
- Een patroon heeft zowel verticale spiegelsymmetrie als (180°-) draaisymmetrie. Moet het dan ook horizontale spiegelsymmetrie hebben?
- Een patroon heeft zowel horizontale spiegelsymmetrie als (180°-) draaisymmetrie. Moet het dan ook verticale spiegelsymmetrie hebben?



afbeelding 9 Horizontale symmetrie-as

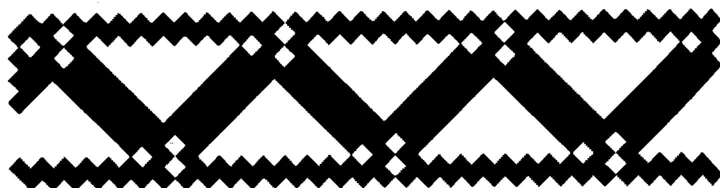


afbeelding 10 Verticale symmetrie-assen



afbeelding 11 Draaisymmetrie

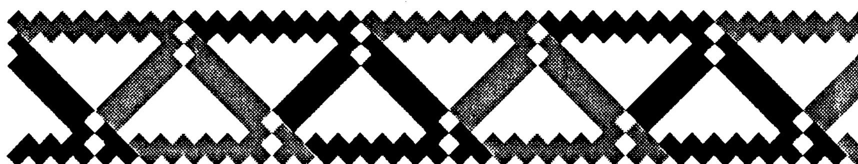
Ook ‘schuifspiegelsymmetrie’ (’voetsporen-symmetrie’ is op leerlingenniveau misschien een duidelijker woord) komt op sipatsi voor.



afbeelding 12

Theoretisch zijn er voor decoratiestroken zeven symmetrie-klassen mogelijk. Sipatsi-vlechters blijken inderdaad decoratiestroken uit alle zeven klassen te ontwerpen.
Een hieruit voortvloeiende vraag voor wiskundeonderwijs is bijvoorbeeld:

- Ontwerp uit iedere klasse één of meer gipatsi-patronen.



afbeelding 13

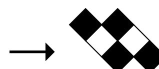
Sipatsi en combinatoriek

Aan een gipatsi-motief kun je dimensies toekennen. De grondvorm van zo’n motief is een gekarteld parallellogram, bestaande uit hokjes, die al dan niet gekleurd zijn. Onderstaand motief heeft dimensies van 8 bij 13, waarbij de eerste dimensie overeenkomt met de periode *p*, en de tweede de ‘diagonale hoogte’ *d* is.

Alle decoratiestroken zijn visueel afgescheiden van de ‘witte’ delen erboven en eronder en hebben dus een ‘zwarte’ rij boven en onder. De overblijvende hokjes kunnen ‘zwart’ of ‘wit’ zijn.

- Hoeveel verschillende gipatsi-patronen bestaan er nu bijvoorbeeld met een motief van 2 bij 3?

De bovenste en onderste rij bestaan in ieder geval uit zwarte hokjes.
De enige vrijheid zit in de rij in het midden:



afbeelding 14

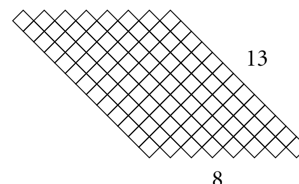
Daarvoor zijn voor het motief in principe vier mogelijkheden, symbolisch aangeduid met zz, zw, wz, ww. Als de hokjes dezelfde kleur hebben (zz of ww), dan ‘degradeert’ het motief tot een motief van 1 bij 3:

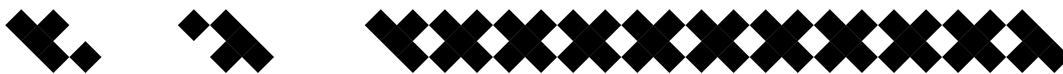


afbeelding 15

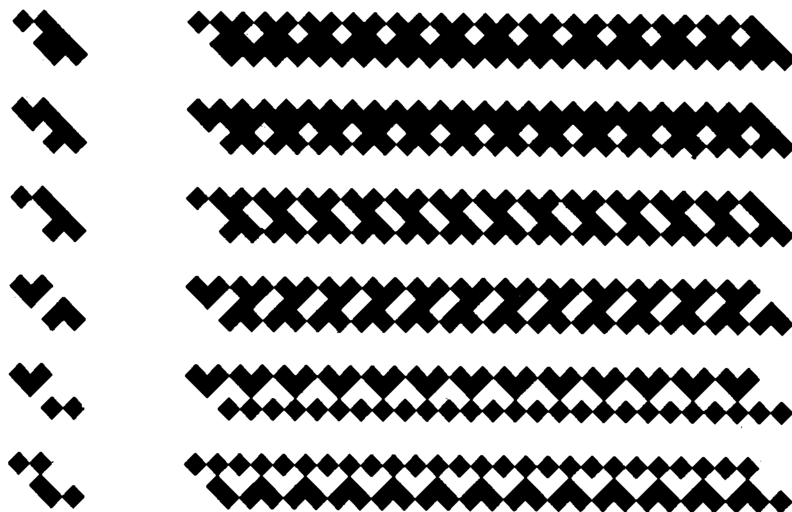
Hebben de hokjes een verschillende kleur, dan zijn er voor het motief nog twee mogelijkheden (zw en wz). Maar beide mogelijkheden leiden tot hetzelfde patroon. (afbeelding 16)

Dus in feite is er maar één patroon dat hoort bij een motief met dimensies 2 bij 3.
In afbeelding 17 staan de zes verschillende gipatsi-patronen die gevormd kunnen worden door een motief van 2 bij 4.





afbeelding16



afbeelding17

Hieraan zouden bijvoorbeeld de volgende vragen gekoppeld kunnen worden.

- Vind alle verschillende gipatsi-patronen met een motief van 3 bij 3.
- Hoeveel gipatsi-patronen bestaan er met een motief van 3 bij 4? Zou je dat aantal ook kunnen vinden zonder te tekenen?
- Kun je een formule vinden voor het aantal gipatsi-patronen met een motief van *p* bij *d*?

Discussie

Zoals hierboven geschetst, vormen sipatsi een aanknopingspunt voor zo uiteenlopende onderwerpen als rekenen, meetkunde en combinatoriek. In didactische zin kunnen we dus spreken van een rijke context. Daarbij komt dat iedere Moçambikaan ze kent. Op de markt zijn ze gemakkelijk verkrijgbaar. Veel leerlingen zullen ooit gezien hebben hoe ze worden vervaardigd. Een deel zal ook de elementaire vlechtregels van huis uit hebben meegekregen. Sipatsi behoren daarom zeker tot de belevingswereld van Moçambikaanse leerlingen. Daar vormen ze mijns inziens een beter startpunt voor wiskundeonderwijs dan stadsplattegronden, dienstregelingen of bedrijfslogo's, om maar eens een paar westerse contexten te noemen.
Nu ging het mij hierboven natuurlijk niet om het aan de man brengen van sipatsi als hèt middel om vervreemding bij Moçambikaanse leerlingen te bestrijden. Het ging om een voorbeeld, een concrete uitwerking van het gedachtengoed van de Etnomathematica. Er zijn meer contexten te vinden. En die kunnen per land, of zo je wilt per cultuur, verschillen.
Of je nu kunt zeggen dat sipatsi-vlechters wiskunde ontwikkelen, daar plaats ik een vraagteken bij. Je kunt misschien zeggen dat ze wiskundig actief zijn, in de zin dat zij iets maken, dat met wiskundige taal te beschrijven valt. Maar zelf maken zij geen gebruik van die taal. En dat is volgens mij nu juist de essentie van wiskunde: wiskundige activiteiten benoemen, expliciet maken, in taal vatten, boven de daad uittillen. Dat wordt niet door de sipatsi-makers gedaan, maar door degenen die hier wiskundeonderwijs uit halen. Bovendien blijkt die wiskunde niet een heel andere dan 'onze' wiskunde, zoals je misschien zou verwachten gezien het uitgangspunt van de Etnomathematica.
Mij kan dit trouwens weinig schelen. Wat ik zie is een rijke context, uit de eigen cultuur, waar meer wiskunde in zit dan je zo op het eerste gezicht vermoedt. Vooral uit psychologisch oogpunt lijkt het me goed dit soort contexten in te zetten bij het wiskundeonderwijs. Een aardig aspect is nog dat sipatsi uitnodigen tot 'materieel handelen', in bijvoorbeeld een wiskundewerklokaal. In ieder geval ben ik zelf aan het vlechten geslagen en daarbij kwam ik er al gauw achter dat dit een hele kunst is.
We moeten wel beseffen dat het vinden van dit soort contexten veel onderzoek met zich meebrengt. In de westerse onderwijswereld is in de loop van de jaren een hele verzameling contexten opgebouwd. Daarbij hebben ontwikkelaars uit de verschillende landen inspiratie uit elkaars vondsten geput, of zo je wilt, vondsten van elkaar gepikt. Het aantal ontwikkelaars in de Derde Wereld is echter een stuk kleiner en bovendien werken zij meestal veel meer geïsoleerd. De Etnomathematica zal het dan ook vooral moeten hebben van de kwaliteit van de gevonden contexten, en niet van de kwantiteit. Het begrip 'eigen cultuur' zou bovendien niet te eng gedefinieerd moeten worden. Ik

Ingezonden

Alternatief voor werkblad

In nummer 72-2 (blz. 108), werkblad tafelkleed, staat een leuke variant op het experimentele examen 1992-I C/D. Als die opgaven gemaakt zijn, zodat iedere leerling zich het naaiprobleem kan voorstellen en bijvoorbeeld weet wat een zoom is, zou ik er echter, na vraag 7, een ander slot aan willen maken. Bij 9 vind je namelijk lapbreedte $127\sqrt{2} \approx 180$ cm. De lap is maar 150 cm breed, haar gewenste kleed lukt zo dus niet.

Mijn versie:

Ans heeft een lange lap van maar 150 cm breed. Ze wil daarom voor het ronde kleed een aantal gelijke sectoren uitknippen en aan elkaar naaien. De symmetrie-as van een sector moet steeds, zoals in de figuur, midden op de lap komen, anders past het patroon niet mooi. Ze naait 1,5 cm van de rand, zie de stippellijntjes.

8 Bereken in cm de straal van de te knippen sectoren.
Als je geen straal vond, gebruik dan verder 123 cm.
Eerst bepaalt ze of het met 4 kwartcirkels lukt.
9 Laat zien dat deze te breed worden voor haar lap.
Ze probeert nu 6 gelijke sectoren.
10 Hoeveel graden wordt de tophoek van zo'n zesde cirkeldeel?
11 Laat zien dat deze delen wel passen.
12 Bepaal hoeveel meter stof ze voor dit kleed nodig heeft, rond af op dm.
Zouden vijf sectoren ook lukken?
13 Zoek dit uit en bepaal met hoeveel minder stoflengte ze dan toe zou kunnen, als het lukt.

De berekening met gonio van 13 is alleen D-stof, maar met tekenen op schaal, met eventueel uitknippen en opplakken, is het hele probleem prachtig op te lossen. Ik heb daarom bewust na 8 geen 'bereken' meer gebruikt om ook de tekenoplosmethode mogelijk te maken. Volgens het nieuwe programma kan de leerling 'zich bedienen van adequate onderzoeks- en redeneerstrategiën'. Ook staat op blz. 35 van de syllabus: …'Daarmee is het oplosproces nog niet voorgestructureerd… Soms wordt de keuze van een oplosweg doelbewust aan de kandidaat overgelaten'.

Na 9 kan natuurlijk ook:
10 Wat is de grootste straal voor een kwartcirkel stof die nog wel op de lap past?
11 Hoever komt het kleed dan van de grond te hangen?

Als de stof geen patroon heeft is het natuurlijk een voordelige oplossing om 2 halve cirkels tegen resp. de linker- en rechterzijkant van de stof te leggen; een mooie vraag om in een latere les te stellen, waarbij misschien meer leerlingen aan het schuiven gaan met geknipte halve cirkels?

Als u iets met deze brief doet, hoor ik graag uw ervaringen!

Agneta Aukema-Schepel, Buitenplaats 77, 8212 AC Lelystad

kan me best voorstellen dat er nauwe samenwerking op dit gebied ontstaat tussen verwante landen, bijvoorbeeld tussen de landen van Zuidelijk Afrika.
Verder moet er rekening mee gehouden worden dat de Derde Wereld in zekere zin verwestert, zeker in de grote steden. Dat betekent dat niet alle contexten uit het Westen per definitie taboe zouden moeten worden verklaard. Er zou nauwkeurig naar de achtergrond van de leerlingen gekeken moeten worden en er zou - hetzelfde geldt overigens ook voor Nederland - verscheidene contexten moeten worden aangeboden, voor elk wat wils.

Terugblik

In de drie artikelen die in deze serie geschreven zijn gaf ik een korte schets van het wiskundeonderwijs in de Derde Wereld. Daarbij lag de nadruk op Afrika, omdat ik daar zelf de meeste banden mee heb. Ook lag de nadruk op lesmateriaal en bijvoorbeeld niet op leraren en hun onderwijsactiviteiten.
In het eerste artikel [3]) beschreef ik de problematiek, waarbij ik de onderzoeken van Gay en Cole [4]) onder de Kpelle in Liberia als introductie gebruikte. Ik gaf wat voorbeelden uit Afrikaanse schoolboeken die helemaal geschreven zijn in de geest van de New Math. Het zijn bijna dezelfde boeken als die wij hier in de jaren zeventig gebruikten, met marginale aanpassingen aan de lokale situatie ('overplakken' noemde ik dat). In het tweede artikel [5]) stond een beknopt portret van 'de' leerling in de Derde Wereld. Ook gaf ik wat voorbeelden uit Afrika van wat wij hier Realistische wiskunde noemen. Dit laatste artikel concentreerde zich op een concrete uitwerking van de ideeën van de Etnomathematica, waarbij de eigen culturele wortels

een inspiratiebron vormden voor aansprekend wiskundeonderwijs.

Met dank aan

Tot slot wil ik nog de volgende personen bedanken die mij bij het schrijven van deze artikelen hulp hebben geboden. Fred Pach (Amsterdam College), voor zijn commentaar op inhoud, spelling en stijl. Kees Smit, Gerard Thijs (beiden van Dienst Ontwikkelingssamenwerking, Vrije Universiteit Amsterdam), Evert van de Vrie (OU) en Ghislain Spaak (INDRAP, Niger) voor het beschikbaar stellen van materiaal.
Voor reacties houd ik me aanbevolen. Ook nodig ik u, en dan met name de lezers met Derde Wereldervaring, bij deze uit om zelf eens een artikel te schrijven. Daarin zouden weer andere aspecten van het wiskundeonderwijs in de Derde Wereld aan de orde kunnen komen.

Noten

1 *Paulus Gerdes en Gildo Bulafo*
Sipatsi The Technology, Art and Geometry in Inhambane
ISP, Maputo, Moçambique (1994)

2 *Marja Meeder en Heleen Verhage*
Regelmaat en symmetrie
Leerpakketje W12-16 (1990)

3 *Hans Wisbrun*
Wiskundeonderwijs in de Derde Wereld (deel 1)
Euclides 71-1 (1995)

4 *J. Gay en M. Cole*
The New Mathematics and an Old Culture
New York (1967)

5 *Hans Wisbrun*
Wiskundeonderwijs in de Derde Wereld (deel 2)
Euclides 71-4 (1996)

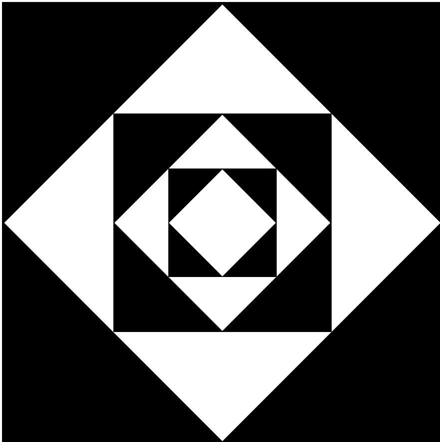
40 jaar geleden

UIT HET VERSLAG VAN DE COMMISSIE VOOR HET STAATSEXAMEN H.B.S. IN 1955
Wiskunde h.b.s. A en B

De commissie wiskunde I constateerde opnieuw, dat de hoedanigheid en de verzorging van het schriftelijke werk nog steeds onvoldoende zijn. De prestaties van vele kandidaten moesten met de cijfers 1, 2 of 3 worden gewaardeerd.
De resultaten van het mondelinge examen vallen, gelet op het onvoldoende schriftelijk werk, niet tegen.
De wenselijke parate kennis betreffende algebraïsche en goniometrische functies, grafische voorstellingen daarvan, goniometrische verhoudingen en trigonometrische formules, is veel groter dan een aantal jaren geleden. Het is de commissie opgevallen, dat een aantal kandidaten wel vrij moeilijke ongelijkheden kan oplossen, maar faalt bij de opgaven van het type $x^2 < 9$.
Ook worden de ongelijkheden $x > 9$ en $x < 3$ vaak gecombineerd tot $3 > x > 9$.
Bij de goniometrie blijkt men de rechthoekige driehoek met de zijden 3, 4 en 5 niet te kennen. Het berekenen van cos x of sin $x = 0{,}8$ is een tijdrovende bezigheid.

De tijd kan beter worden benut om het examen op hoger niveau te brengen. Bij de correctie van het schriftelijke werk voor stereometrie en beschrijvende meetkunde viel het op, dat vele kandidaten geen onderscheid maakten tussen lijn (of rechte), halve lijn (of halve rechte) en lijnstukken.
Ook meenden nog vele kandidaten, dat als vlak V loodrecht staat op vlak W, elke lijn in V loodrecht staat op elke lijn in W.
Bij mondelinge examens bleek, dat vele kandidaten niet in staat waren definities en stellingen correct te formuleren.
In de beschrijvende meetkunde verdient het aanbeveling, dat een raaklijn uit een punt buiten een cirkel aan die cirkel ook werkelijk geconstrueerd wordt en niet wordt verkregen door een lineaal langs de cirkelomtrek te leggen. Het is zeer gewenst, dat constructies van een korte toelichting worden voorzien, waarbij de gebruikte punten, lijnen en vlakken met letters worden aangeduid en in de toelichting worden vermeld.
Bij de mondelinge examens beschrijvende meetkunde bleek bij de kandidaten vele malen een tekort aan routine in de eenvoudigste grondconstructies, zodat zij aan het uitwerken van een eenvoudig vraagstuk nauwelijks toekwamen. **Uit: Euclides 32 (1956-1957)**

Werkblad



Vierkant

Hiernaast staat het logo afgebeeld van de stichting VIERKANT.
Stel dat het witte vierkantje in het midden een oppervlakte heeft van 1 cm^2.

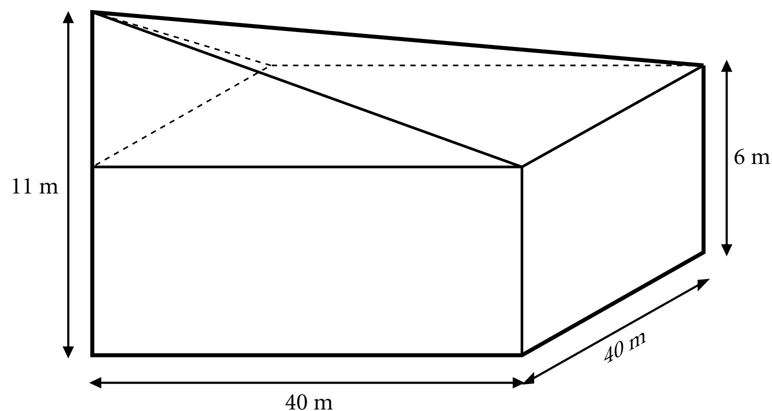
22 Hoeveel cm^2 is de oppervlakte van het totale witte gedeelte van dit logo?

De stichting VIERKANT wil dit logo op een groot uithangbord zetten. Alle zijden moeten daartoe met 15 worden vermenigvuldigd.

23 Bereken hoe groot de oppervlakte van het zwarte gedeelte van dit logo dan wordt.

Kerk

Hieronder zie je een schetsmatige tekening van de kerk van Zwolle-Zuid.
De afstanden zijn in meters.



9 Bereken de inhoud van deze kerk.

Geref. S.G. prof.dr. S. Greijdanus, mavo-4 schoolonderzoek.

Werkblad

Het wonder uit de kraan

In de folder van een waterleidingmaatschappij staat het volgende:

De Waterleiding Maatschappij Overijssel N.V. levert jaarlijks zo'n 64 miljard liter water aan ruim een kwart miljoen huishoudens, bedrijven en instellingen in 45 gemeenten.

1 Hoeveel meter is de ribbe van een kubusvormige bak met een inhoud van 64 miljard liter? Schrijf je berekening op.

Een lekkende kraan die tien druppels per minuut laat vallen, verspilt jaarlijks *tweeduizend liter* water. Een doorlopend toilet nog veel meer. Jammer, het is zo gemakkelijk en goedkoop te verhelpen.

2 Bereken in hoeveel tijd zo'n lekkende kraan één liter water verspilt. Schrijf de berekening op.

In de folder is een cilindervormig bad getekend met een man erin.



Je kunt je afvragen of de tekenaar met dit bad een hoeveelheid van 2000 liter water goed heeft weergegeven.

volume bad $= \pi r^2 \times h$

3 Kies een hoogte h en een straal r die bij het bad passen en toon dan met een berekening aan of de tekenaar wel of niet een juist beeld geeft van 2000 liter water.

—

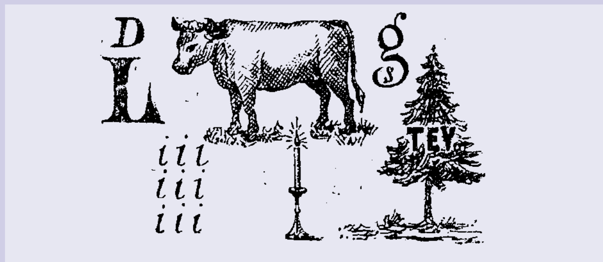
Examen vbo-mavo-D 1996, tijdvak 2, experimenteel

Opgave 674

Recreatie


WAAR IS ZIJN VROUW?

Vorig jaar, in Recreatie 667, schreef ik dat er bij de boekenclubs een puzzelboek verschenen was: 'Optische Illusies en andere Puzzels'. Onlangs is het vervolg verschenen: 'Spiegeleffecten en andere verborgen Illusies' van Jack Botermans en Jerry Slocum. (ISBN 90 67 61 2715). De prijs is wederom ƒ 19,90. In de clubcatalogus wordt het aangekondigd met: 'Niets is wat het lijkt! Hoe uw ogen u voor de gek kunnen houden …'. Inderdaad kom je m.b.v. het ingesloten spiegelvel tot verrassende ontdekkingen. Door van dit vel een spiegelkoker of spiegelkegel te maken ontstaan er fraaie ANAMORFOSEN! Door het vel als vlakke spiegel te gebruiken ontstaan er weer andere effecten. De historische zoekplaten e.d. zijn weer afkomstig uit de puzzelcollectie van Jerry Slocum. Toch zou ik het leuk vinden, ik heb het vorig jaar ook al geschreven, als de historische sigarenzakjes óók eens gepubliceerd zouden worden. Als u, lezer, informatie hierover hebt, dan houd ik mij ten zeerste aanbevolen, want er is zeer weinig over dit onderwerp bekend. Op deze pagina een paar voorbeelden uit de dertiger jaren:



Na dit boek vol raadsels en zoekplaatjes deze maand een wiskundig zoekraadsel! Ik zoek een functie $f(x)$, waarbij $x \in \mathbb{R}$, behalve $x = 0$ en $x = 1$. Hij voldoet voor elke $x \in D_f$ aan

$$f(x) + f(1 - \frac{1}{x}) = x$$

Welke functie $f(x)$ zit hierin verborgen?

Bij juiste oplossing ontvangt u 5 punten voor de puzzelladder, mits binnen 1 maand ingezonden na verschijning.

Oplossingen, nieuwe opgaven en correspondentie over deze rubriek aan

Jan de Geus
Valkenboslaan 262-A
2563 EB Den Haag.

Oplossing 671

10	56	6	43	8	55	32	45
5	42	9	56	31	44	15	54
58	11	30	7	16	53	46	33
41	4	17	12	47	34	25	14
18	59	40	29	24	13	52	35
1	62	3	48	51	36	23	26
60	19	64	39	28	21	50	37
63	2	61	20	49	38	27	22

Hans Verdonk (38), Den Haag

Q	w	S	J	G	B	M	J
T	I	P	v	L	I	F	C
x	R	t	H	**A**	N	K	H
s	U	y	O	u	j	D	E
z	a	r	V	n	Z	G	i
q	d	o	&	k	E	D	Y
b	&	f	m	W	B	h	F
e	p	c	A	g	l	X	C

Pieter Torbijn (48), Den Haag

I	B	G	B	Y	y	W	&
F	C	J	C	V	A	Z	x
A	H	U	D	l	X	x	H
T	E	D	j	F	I	w	&
f	q	S	m	d	k	G	J
R	n	e	E	i	M	a	v
r	g	p	P	t	c	K	N
o	Q	s	h	L	O	u	b

M. Roos-Rietdijk (20), Alphen a/d Rijn

t	g	C	y	v	B	O	&
D	E	u	C	B	z	w	**A**
f	s	h	L	x	P	A	N
F	E	D	I	i	M	J	Q
r	e	G	F	K	R	j	V
Z	b	J	S	H	W	m	I
d	g	&	X	G	o	U	k
a	Y	c	p	T	l	H	n

Harm Bakker (62), Marum

I	c	z	o	Y	a	x	m
&	p	J	b	y	n	X	&
d	H	A	q	M	Z	l	w
B	**A**	e	U	D	r	N	W
G	T	C	L	I	V	v	k
B	f	D	E	s	K	H	O
S	F	h	J	Q	F	j	u
g	C	R	E	i	t	P	G

Dick Buijs (55), Kerk-Avezaath

R	C	F	f	T	j	m	h
G	N	S	D	E	g	b	k
B	Q	e	U	c	l	i	n
M	H	O	D	E	s	I	a
P	A	V	d	J	x	o	t
I	L	C	w	r	F	&	H
&	W	J	**A**	y	Y	u	p
K	B	z	X	v	q	G	Z

Floor van Lamoen (67), Goes

S	P	f	q	G	N	h	F
e	r	R	O	g	E	F	M
Q	T	d	H	p	L	G	i
w	I	s	K	u	n	D	E
U	c	v	o	C	D	j	H
&	x	J	t	m	A	Z	C
b	V	z	B	&	X	I	k
y	A	a	W	J	l	B	Y

Floor van Lamoen (67), Goes

In de grote vakantie is er door vele lezers met de schaakpaarden gesprongen. Bij de getallen moesten de kwadraten in een vierkant staan. De paardesprongen zijn allemaal gesloten. Bij de letters zijn ingevuld: hoofdletters & kleine letters & hoofdletters. De beginletter **A** is steeds vetgedrukt. *Pieter Torbijn* wist zelfs te maken: I THANK YOU, DE G.

Voor tien extra bonuspunten wisten verschillende lezers EUCLIDES op het bord te krijgen. Doordat een paard bij elke sprong van kleur wisselt is EUCLIDES op een rij, kolom of diagonaal onmogelijk. De mooiste inzendingen vindt u hier met de complimenten van de puzzelredacteur.

Met 67 punten is deze maand winnaar van een boekenbon van *f* 25,–:

Floor van Lamoen
Stoofstraat 25
4461 CB Goes

Heel hartelijk gefeliciteerd!

KALENDER

Euclides verschijnt dit schooljaar nog op 15 januari, 15 februari, 15 maart, 30 april en 15 juni.

In deze kalender kunnen alle voor wiskundedocenten toegankelijke en interessante bijeenkomsten worden opgenomen. Data melden bij de hoofdredacteur uiterlijk twee maanden voor de verschijningsdatum. Dit kan ook via e-mail:

hoogland@rulwinw.leidenuniv.nl

APS-hoorzitting Wiskunde in 4 havo/4 vwo
do. 12 december 1996
APS: 030 - 2856722

Studiedag resultaten experiment grafische rekenmachine
wo. 18 december 1996 in Zwolle
Organisatie RU Groningen:
050 - 3637121
(Marga Witterholt)
Wat hebben de leerlingen beter of minder goed geleerd?

Wintersymposium
za. 4 januari 1997
Wiskundig Genootschap
Zie aankondiging blz. 133

Nationale Wiskunde Dagen
vr. 31 januari/za. 1 februari 1997
Freudenthal instituut:
030 - 2611611
Zie aankondiging blz. 19

Regionale bijeenkomsten
11 maart 1997 Zwolle
13 maart 1997 Leiden
18 maart 1997 Eindhoven
(onder voorbehoud)
NVvW: 0411 - 673468
Aankondiging volgt later

Lezingenserie Hogeschool van Utrecht
ma. 3 maart 1997: 20.00 u
HvU: 030 - 2547230
Prof.dr. Ferdinand Verhulst: Denken en rekenen over atmosferen en oceanen.

Kangoeroe-wedstrijd
vr. 21 maart 1997
TUE: 040 - 2472738
Aankondiging volgt later

Eerste ronde Wiskunde Olympiade
vr. 11 april 1997
Secret.: 026 - 3521294
Aankondiging volgt later

APS-conferentie Grafische rekenmachine
wo. 16 april 1997
APS: 030 - 2856722
Zie advertentie 72-2

APS-conferentie Schoolonderzoek vbo/mavo
wo. 23 april 1997
APS: 030 - 2856722
Zie advertentie 72-2

Lezingenserie Hogeschool van Utrecht
wo. 18 juni 1997: 20.00 u
HvU: 030 - 2547230
dr. Marjolijn Witte: Het geslacht van de wiskundeknobbel.

Internet WWW-sites voor wiskundedocenten:

Eisenhower National Clearinghouse
http://www.enc.org

Freudenthal instituut, wisweb
http://www.fi.ruu.nl/wisweb/nl

Freudenthal instituut, verwijzingen
http://www.fi.ruu.nl/nl/link

Amerikaanse Vereniging van Wiskundeleraren:
http://www.NCTM.org

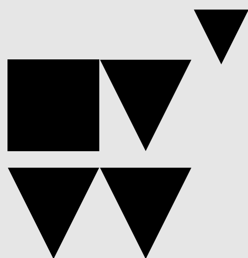
Software-evaluaties:
http://bve-scennet.dds.nl

SLO-lijn / School van Morgen:
http://192.87.215.10

Digitale school:
Zie blz. 132

Docenten met e-mail kunnen een berichtje sturen aan Jos Andriessen. Die onderzoekt mogelijkheden om tot een e-mail netwerk te komen:

Andriess@worldonline.nl



Nederlandse
Vereniging van
Wiskundeleraren

OPROEP
nieuwe redacteuren

Een uitdaging voor u?

Omdat een aantal leden de redactie van Euclides gaat of heeft verlaten zoekt Euclides met ingang van **1 januari 1997 nieuwe redacteuren (m/v).**

We zijn speciaal op zoek naar redacteuren die artikelen kunnen (doen) schrijven over software en informatietechnologie.
Verder zoeken we ook met name docenten die werkzaam zijn in het vbo/mavo om er voor te zorgen dat de ontwikkelingen daar goed in Euclides aan bod komen.
Ook zoeken we versterking van de kernredactie om de kwaliteit van het blad en de artikelen mede te bewaken.

De redactie vergadert minimaal drie keer per jaar, de kernredactie minimaal drie keer per jaar extra.

De redactie roept belangstellenden op zich te melden bij de voorzitter van de redactie:

G. Zwaneveld
Bieslanderweg 18
6213 AJ Maastricht
tel. 043-3256413

EUCLIDES

Bij hem kan ook het redactiestatuut worden opgevraagd. In dit statuut staan onder andere de taakomschrijvingen van de redacteuren.

Nieuwe redacteuren worden benoemd door het bestuur van de Nederlandse Vereniging van Wiskundeleraren op voordracht van een commissie waarin de hoofdredacteur, de voorzitter van de redactie en een vertegenwoordiger van het bestuur zitting hebben.

Voor het nieuwe examen

Opgaven wiskunde vbo-mavo/cd

Dit schooljaar worden de eerste landelijke examens vbo-mavo volgens het nieuwe leerplan afgenomen. Wilt u uw leerlingen grondig voorbereiden op het nieuwe cd-examen of op het schoolonderzoek, dan kunt u nu beschikken over *Opgaven wiskunde vbo-mavo/cd*.



Werkboek

Bij de nieuwe examens wordt gewerkt met werkvellen; ook daarmee zullen de leerlingen moeten leren omgaan. Daarom zal naast de opgavenbundel een *Werkboek* verschijnen.

De *Opgaven wiskunde vbo-mavo/cd* en *Werkboek* zijn ontwikkeld in samenwerking met het Algemeen Pedagogisch Studiecentrum. Zij zijn bruikbaar naast elke methode.

Ook verkrijgbaar via de boekhandel

Bestellen

Opgaven wiskunde vbo-mavo/cd
ISBN 90 01 09018 4 112 p ƒ 29,70

Werkboek
ISBN 90 01 80593 0 25 p ƒ 9,95

Wolters-Noordhoff
Postbus 58
9700 MB Groningen
Telefoon (050) 522 63 11

Wolters Noordhoff

420/6439-96